Tommi Marjomaa

Identiteetin- ja pääsynhallintapalvelun tuotteistaminen

Asiakastarpeiden selvittäminen ja tuotteiden soveltuvuuden varmistaminen

Metropolia Ammattikorkeakoulu

Tradenomi

Liiketalouden tutkinto-ohjelma

Opinnäytetyö

Helmikuu 2018

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Tommi Marjomaa Identiteetin- ja pääsynhallintapalvelun tuotteistaminen 42 sivua + 3 liitettä Helmikuu 2018
Tutkinto	Tradenomi
Koulutusohjelma	Liiketalouden tutkinto-ohjelma
Suuntautumisvaihtoehto	
Ohjaaja(t)	Lehtori Pirjo Elo

Yrityksen menestykselle on tärkeää, että sen tavoitteena on aidon lisäarvon tuottaminen asiakkaille. Asiakaslähtöinen toiminta on perusta kestäville asiakassuhteille ja hyville tuloksille. Lisäksi asiakaslähtöisyys tukee yrityksen uudistumista ja innovointia. Kun yrityksissä kehitetään uusia palveluita asiakaslähtöisesti, tarkoittaa se, että asiakasnäkökulma otetaan huomioon uuden palvelun suunnittelussa. Sen yhtenä osana on asiakastarpeiden selvittäminen. Näin varmistetaan, että palvelulla vastataan näihin tarpeisiin. Opinnäytetyön toimeksiantaja Citrus Solutions Oy oli tehnyt havaintoja asiakkaiden tarpeista, joihin ratkaisu voisi olla identiteetin- ja pääsynhallintapalvelu.

Tämä toiminnallinen opinnäytetyö oli osa toimeksiantajan asiakaslähtöistä identiteetin- ja pääsynhallinnan tuotteistamisprojektia. Tarkoituksena oli tuottaa toimeksiantajalle selvitys asiakastarpeista ja toimeksiantajan alustavasti valitsemien tuotteiden soveltuvuudesta vastaamaan havaittuihin asiakastarpeisiin.

Työn teoreettisessa osuudessa tutustuttiin ensin tuotteistamisprosessiin ja sen eri vaiheisiin, jonka jälkeen sukellettiin identiteetin- ja pääsynhallinnan kokonaisuuteen. Teoreettisen viitekehyksen lähteinä käytettiin pääasiallisesti ammattikirjallisuutta ja tutkimuksia. Niiden lisäksi lähdemateriaalina käytettiin internetlähteitä, jotka käsittelivät tuotteistamista sekä identiteetin- ja pääsynhallinnan kokonaisuuteen liittyviä osa-alueita, kuten käyttäjän luotettava tunnistaminen, kertakirjautuminen, keskitetty lokienhallinta ja luottamusverkostot.

Opinnäytetyön tuloksena syntyi selvitys, jota toimeksiantaja voi hyödyntää tuotteistamisprojektissaan. Selvityksen sisältö koostui asiakastarpeista tehdyistä havainnoista ja millä tavalla näihin tarpeisiin voitiin vastata.

Johtopäätöksissä todettiin, että toimeksiantajan alustavasti valitsemilla ratkaisuilla oli mahdollista vastata suureen osaan havaituista asiakastarpeista. Tämän lisäksi toimeksiantajan nykyiset palvelut tukivat hyvin tuotteistamisen alla olevaa kolmitasoista identiteetin- ja pääsynhallinnan palvelua.

Avainsanat	asiakastarpeet, henkilötieto, identiteetinhallinta, kertakirjautuminen, käyttövaltuushallinta, pääsynhallinta, tuotteistaminen

Author(s) Title Number of Pages Date	Tommi Marjomaa Productisation of Identity and Access Management 42 pages + 3 appendices February 2018
Degree	Bachelor of Business Administration
Degree Programme	Economics and Business Administration
Specialisation option	
Instructor(s)	Pirjo Elo, Senior Lecturer

For a company to succeed, it is important that its goal has to be in generating genuine added value for customers. Customer-oriented operations serve as a basis for long lasting customer relationships and good results. In addition, customer orientation supports the company's renewal and innovation. When companies want to develop new services in a customer-oriented way, it means that the customers' perspective must be taken into account when designing a new service. One part of it is to identify the customer's needs. This ensures that the new service can meet these needs. The thesis was commissioned by a company called Citrus Solutions Oy, which has made observations on customer needs. Those needs could be solved with an identity- and access management service.

The purpose of the project based thesis was to clarify the customer needs and ensure that the initially selected software by the company are suitable to match the customer needs. This will be made as part of the customer's customer-oriented identity and access management productisation.

The theoretical part of the thesis clarifies first the productisation process and its various phases. After that the overall picture of identity and access management are looked into. The sources of the theoretical framework were mainly professional literature and studies. In addition, some source material consisted of Internet sources dealing with productisation, as well as items related to identity and access management, such as user authentication, single sign-on, log management and trust federations.

The outcome of the project is a report the company can use in their ongoing productisation project. The report consists of identified customer needs and proposal for how those needs can be met.

The conclusion is that the customer's initially selected solutions are able to meet a large part of the identified customer needs. In addition to this, the existing service offerings of the company are suitable for supporting the three-tier identity and access management service which the company is productising.

Keywords	customer needs, personal data, identity management, single sign-on, user rights management, access management, productisation

Sisällys

1 Johdanto

Opinnäytetyön tarkoituksena on osana identiteetin- ja pääsynhallintapalvelun tuotteistamisprojektia tuottaa selvitys asiakastarpeista ja varmistaa alustavasti valittujen ohjelmistotuotteiden soveltuvuus vastaamaan näihin asiakastarpeisiin. Opinnäytetyön tavoitteena on, että toimeksiantaja voi hyödyntää valmistuvaa selvitystä tuotteistamisprojektissaan.

Lähtökohta opinnäytetyölle on toimeksiantajan halu tuottaa asiakasnäkökulman huomioiva palvelu, joka luo asiakkaille lisäarvoa ja mahdollistaa toimeksiantajalle taloudellisesti kannattavaa liiketoimintaa. Identiteetin- ja pääsynhallintapalvelun tavoitteena on täyttää muun muassa kuntien toimintaa ohjaavaan Sote-muutoksen ja EU:n tietosuoja-asetuksen asettamat vaatimukset.

Opinnäytetyön toimeksiantaja on Citrus Solutions Oy. Yritys on digitaalisten palveluiden toimittaja. Vuonna 1993 perustettu yritys työllistää tällä hetkellä viitisenkymmentä työntekijää. Nykyistä nimeä yritys on käyttänyt vuodesta 2009 saakka ja sillä on toimipaikat Helsingissä ja Turussa. Citruksen palveluihin kuuluvat asiantuntijapalvelut, sekä räätälöityinä ratkaisuina että täysin tuotteistettuina SaaS-palveluina.

Toimeksiantaja on päätynyt alustavissa selvityksissään Micro Focuksen ohjelmistoihin, joita saa paikallisesti asennettavina versioina ja pilvipohjaisina SaaS-palveluina (Software as a Service). SaaS-palveluiden ominaispiirteisiin kuuluu se, ettei asiakaskohtaisia tuotantoympäristöjä ole vaan sama tuotantoympäristö palvelee useampaa asiakasta. SaaS-palvelun toimittaja vastaa esimerkiksi järjestelmän ylläpidosta, tietoturvasta ja tuotantoympäristöstä. SaaS-palveluiden käytöstä maksetaan yleensä käytön laajuuden mukaiset palvelumaksut. (Gibbs 2015.)

Opinnäytetyön aiheena oleva identiteetin- ja pääsynhallintapalvelu on ajankohtainen aihe tietoturva-asioiden piirissä (Nikols 2017). Käyttäjien tarvitsemien käyttäjätunnusten ja salasanojen määrä kasvaa jatkuvasti ja näköpiirissä ei ole hidastumista (Le Bras 2017). Monilla meillä on useita eri käyttäjätunnuksia ja salasanoja sekä töissä että työajan ulkopuolella käytössä oleviin palveluihin. Identiteetin- ja pääsynhallintapalvelun

avulla on mahdollista yhdellä tunnistautumisella käyttää useita eri järjestelmiä ja palveluita niin, ettei jokaiseen järjestelmään tarvitse kirjautua erikseen.

Tietoturva ja erilaiset tietoturvaratkaisut ovat nykytietoyhteiskunnassa erittäin tärkeässä asemassa. Viimeistään toukokuussa 2018 sovellettavaksi tuleva EU:n tietosuoja-asetus pakottaa yritykset parantamaan tietoturvakäytäntöjään (Savolainen 2014).

Tietoturvaratkaisut ovat minulle tuttuja työni kautta. Olen toiminut yli viidentoista vuoden ajan erilaisissa IT-tehtävissä. Tarkoitukseni on hyödyntää opintojen lisäksi työkokemustani palveluntuotteistamisen mahdollisuuksia tutkiessani. Koska minulla ja toimeksiantajalla ei ole aiempaa yhteistä historiaa, pystyn selvittämään asiakastarpeet ja tarkastelemaan valittuja tuotteita ja niiden soveltuvuutta puolueettomasti.

Opinnäytetyön teoriaosuudessa käydään läpi tuotteistamisen sekä identiteetin- ja pääsynhallinnan perusteita. Teoriaosuudessa on otettu huomioon, että kyseessä on ohjelmistotuote, jonka tehokas tuotteistaminen luo yritykselle mahdollisuuden saavuttaa kustannustehokkuutta ja kilpailuetua. Vain fyysisten tuotteiden tuotteistamiseen soveltuvat teoriat on jätetty tarkoituksella pois.

Opinnäytetyö on toiminnallinen opinnäytetyö, joka on rajattu asiakastarpeiden selvittämiseen ja alustavasti valittujen ohjelmistotuotteiden soveltuvuuden varmistamiseen. Opinnäytetyön lopputuloksena valmistuu selvitys päätöksenteon pohjaksi. Selvitystä varten kerätään tietoa laadullisella menetelmällä sekä käyttämällä alan tutkimuksia ja kirjallisuutta. Haastattelut suoritetaan palvelun potentiaalisten asiakkaiden, ohjelmistotoimittajan sekä toimeksiantajan henkilöstön kanssa.

2 Tuotteistaminen

Tuotteistamiselle ei ole olemassa yleisesti hyväksyttyä määritelmää. Tästä johtuen tuotteistamisesta ja siihen liittyvistä toimista käytetään usein muitakin nimityksiä kuten palvelujen konseptointi tai systematisointi. Lisäksi tuotteistamisella voidaan tarkoittaa palvelun vakioimista tuotteen tapaiseksi, täysin vakioiduksi hyödykkeeksi. (Jaakkola & Orava & Varjonen 2009, 1.) Kolmivuotisen LEAPS (Leadership in the Productisation of Services) -tutkimusprojektin tavoitteena oli luoda asiakaslähtöinen ja osallistava tuotteis-

tamisen malli (Tuominen & Järvi & Lehtonen & Valtanen & Martinsuo 2015, 11). Projektissa tuotteistamisen kuvattiin olevan palvelun ja sen tarjoaman arvon kiteyttämistä kuvaamalla ja vakioimalla eri osat (Tuominen ym. 2015, 5). Apusen (2010,13) mukaan tuotteistamisella pyritään luomaan tuote, joka ratkaisee asiakkaan polttavan ongelman, on helppo ostaa ja helppo käyttää.

Tuotteistamisella voidaan tarkoittaa myös uusien tai olemassa olevien palvelujen määrittelyä sekä ainakin osittaista vakiointia. Se voidaan kohdistaa yrityksen sisäisiin ja asiakkaille näkyviin prosesseihin. Tavoitteena on palveluliiketoiminnan kehittäminen ja uudistaminen siten, että kannattavuus paranee ja asiakas saa palvelusta maksimaalisen hyödyn. (Jaakkola ym. 2009, 1.) Sipilän (1996, 12–13) mukaan tuotteistuksesta on kyse, kun palveluista kehitetään selkeitä palvelukokonaisuuksia, joita tarjotaan asiakkaille sellaisenaan tai asiakaskohtaisesti räätälöityinä. Tuomisen ym. (2015, 14) mukaan tuotteistamisen tavoite on luoda yhteinen ymmärrys palvelusta sekä sen luomasta arvosta.

Järjestelmällisen palvelujen kehittämisen tavoite on luoda kannattavaa, innovatiivista ja kilpailukykyistä liiketoimintaa. Lähtökohtana palvelujen kehittämiselle on yrityksen liiketoimintastrategia. (Jaakkola ym. 2009, 1.) Liiketoimintastrategian keskiössä on ajatus, että päivittäinen kilpailu käydään liiketoimintatasolla. Menestyksen kannalta on keskeistä, että yritys voi liiketoimintastrategiallaan luoda kilpailuetua valitsemillaan liiketoiminta-alueilla. (Kamensky 2008, 25.) Sipilä (1996, 34) lisää, että tuotekehityksen on pohjattava liiketoimintastrategian lisäksi markkinoinnin strategiaan. Yrityksellä tulee olla selvä käsitys siitä, mitä palveluja se haluaa ja mitä sen kannattaa tuottaa. (Sipilä 1996, 34.)

Yrityksen liiketoimintastrategiaa määrittävät keskeiset kysymykset liittyvät tavoiteltaviin asiakkaisiin ja asiakassuhteisiin, tuotteisiin ja niiden tuottamiseen, lisäarvon tuottamiseen ja siihen mikä on erikoistumisen, tuotekehityksen ja osaamisen aste. Liiketoimintastrategian tulee myös vastata kysymykseen, onko yrityksellä sellaiset resurssit, että lisäarvoa voidaan tuottaa kilpailukykyisesti. Yrityksellä tulee olla osaamista asiakkaiden, palvelun ja toimialan suhteen. (Jaakkola ym. 2009, 3; Kamensky 2008, 26.) Tuotteistaminen saattaa osoittaa osaamispuutteita, jotka voidaan ratkaista kehittämällä uutta osaamista, joko sisäisesti tai hankkimalla osaamista yrityksen ulkopuolelta (Sipilä 1996, 36).

Ilman asiakkaita ei yksikään tuote tai palvelu tuota tuloja. Ilman tuloja ei ole liiketoimintaa. Kehittämishankkeiden päätarkoituksena on mahdollistaa palvelut, jotka asiakkaiden mielestä tuottavat heille houkuttelevaa lisäarvoa. Jotta yritys ymmärtäisi asiakkaiden tarpeet ja odotukset, on usein suotavaa osallistaa asiakkaat uuden tuotteen tai palvelun kehittämiseen. (Edvardsson & Olsson 1996, 141–142.) Asiakaslähtöinen kehitystyö ei tarkoita samaa kuin asiakasvetoinen kehitystyö (Jaakkola ym. 2015, 3). Asiakasvetoisessa kehitystyössä asiakas on aloitteellinen kehitystyön tilaajana. Asiakaslähtöisessä kehittämisessä lähtökohtana on asiakastarpeisiin vastaaminen ja arvon tuottaminen asiakkaalle. (Jaakkola ym. 2015, 10–11.)

Osallistamalla asiakkaat yritys voi lisäksi varmistaa, että palveluun saadaan kiteytettyä paras ymmärrys palvelun tuottamasta arvosta (Tuominen ym. 2015, 5). Tuotteistamisen tarkalla ennakkosuunnittelulla pyritään pienentämään epäonnistumisen riskiä ja varmistamaan, että kehittämishankkeen tuloksena tuotetut palvelut todella vastaavat asiakkaiden tarpeita ja tuottavat heille arvoa. (Kinnunen 2004, 96-97.)

2.1 Tuotteistamisprosessi

Tuotteistamisprosessista on olemassa erilaisia malleja ja se voi edetä eri tavoin. Sen muoto voi olla esimerkiksi perinteinen, iteratiivinen tai ketterä. Perinteisessä, vaiheittaisessa mallissa tuotteistaminen koetaan kertaluonteisena tapahtumana, joka etenee vaiheesta toiseen suoraviivaisesti. Iteratiivisessa mallissa palvelun tuotteistaminen tehdään vaiheittain. Sen lisäksi palvelu suunnitellaan jo lähtökohtaisesti sellaiseksi, että sitä voidaan jatkuvasti kehittää. Ketterää mallia käytetään usein silloin, kun palvelutuote halutaan markkinoille nopeasti. Palvelua aletaan usein myydä tuotteistamisprosessin ollessa vielä kesken, ja palvelun jatkokehitys tehdään ensimmäisten asiakkaiden kanssa yhteistyössä. (Tuominen ym. 2015, 10–11.)

Kuten edellä on jo mainittu, niin tuotteistamisprosessin ei tarvitse olla lineaarinen prosessi. Joitakin vaiheita voidaan toteuttaa samanaikaisesti. Yrityksillä on keskenään erilaiset syyt ja tavoitteet tuotteistamiselle. Tämän vuoksi yritykset sekä suunnittelevat että toteuttavat kehittämishankkeensa omista lähtökohdistaan. (Jaakkola ym. 2009, 5.)

Asiakaslähtöistä tuotekehitysmallia tutkittaessa on päädytty kahteen kymmenvaiheeseen malliin. Toisessa edetään vaiheesta toiseen järjestelmällisesti. Toisessa osa vaiheista suoritetaan rinnakkaisesti, jotta palvelun kehittämiseen vaadittavaa aikaa voidaan

lyhentää. (Alam & Perry 2002, 524–525.) Tutkimuksessa todettiin lisäksi, että asiakkaiden osallistaminen on tärkeintä ideoinnissa, palvelun suunnittelussa ja palvelun testaamisessa (Alam & Perry 2002, 533).

Parantainen luokittelee tuotteistamisprosessille kaksi päävaihetta, jotka ovat lupaus- ja lunastusvaihe. Lupausvaiheessa yritys lupaa ratkaista jonkin asiakkaalla olevan todellisen ongelman. Lunastusvaiheessa tehdään kyseisen ongelman ratkaisevan palvelun vaatimusmäärittely. (Parantainen 2007, 134.)

Sipilä taas luokittelee tuotteistamisprosessille viisi minimivaihetta, jotta tuotteistaminen ylipäätänsä voisi onnistua. Tuotteistaminen alkaa tuotevalikoiman analysoinnilla ja suunnittelulla, jonka tuloksena syntyy tuoteluettelo. Tämän jälkeen täsmennetään tuotteistusohjelma ja laaditaan tuotteistussuunnitelma. Tuotteistamisprosessin lopuksi laaditaan hinnoittelustrategia. (Sipilä 1996, 124.)

2.1.1 Palvelutarjooman määrittely ja asiakastarpeiden tunnistaminen

Kehitystyö voidaan aloittaa määrittämällä yrityksen palvelutarjooma eli yrityksen tarjoamien palvelujen kokonaisuus. Palvelutarjooman kuvaamisen ja arvioimisen kautta on mahdollista saada ymmärrys mistä yrityksen liiketoiminta arviointihetkellä koostuu. Tämän jälkeen yritys voi määritellä tavoitteellisen palvelutarjooman, jota tavoitellaan pidemmällä tähtäimellä, esimerkiksi viiden vuoden päästä. Vertailemalla nykyistä palvelutarjoomaa yrityksen liiketoimintastrategiaan ja yrityksen tavoitteisiin voidaan selvittää, millä tavalla liiketoimintaa tulisi uudistaa ja kehittää. (Jaakkola ym. 2009, 7.)

Yrityksen tulee jatkuvasti kehittää palvelutarjoomaansa vastaamaan markkinoiden ja asiakkaiden muuttuvia tarpeita, jopa niitä ennakoiden. Yritysten tulisi pyrkiä havaitsemaan myös markkinoiden piilevät tarpeet ja mahdollisuudet ennen kuin suurin osa asiakkaista on tiedostanut ne. (Andersson ym. 2006, 4; Rissanen 2006, 112.) Koska asiakkaat eivät ole aina selvillä tarpeistaan, tulee palveluntarjoajan selvittää tilanne asiakkaalle ja osoittaa asiantuntemuksensa avulla ne ongelmat, jotka asiakas voi palvelun avulla poistaa (Kinnunen 2004, 42). On kuitenkin huolehdittava, että linkki palvelujen, liiketoimintastrategian ja tavoiteltavien asiakasryhmien välillä on selvä. Uusien palveluiden on sovittava yrityksen liiketoimintastrategiaan. (Jaakkola ym. 2009, 8.)

Tuotteistamisprosessissa voidaan lähteä liikkeelle peruskysymyksistä, jotka liittyvät asiakkaisiin, henkilöstöön ja yrityksen tavoitteisiin. Peruskysymykset liittyvät siihen, miten yritys voi tarjota palveluitaan aiempaan verrattuna tehokkaammin tai paremmalla katteella. Odotusten määrittämiseksi tulee tuntea asiakkaan ongelma, jonka ratkaisemiseen pyritään. (Apunen 2010, 20–21.)

Mark Cook kehottaa käyttämään seuraavia kysymyksiä ongelman määrittelyvaiheessa selvittämään, ollaanko ratkomassa asiakkaan näkökulmasta relevanttia asiaa: Tunnistavatko asiakkaat, että heillä on ongelma, jota yritetään ratkoa? Jos kyseiseen ongelmaan olisi ratkaisu, ostaisivatko he sen? Ostaisivatko he ratkaisun meiltä? Voimmeko rakentaa ratkaisun ongelmaan? Usein tuotekehityksessä hypätään suoraan viimeiseen kysymykseen ja rakennetaan ratkaisu ilman todellisen ongelman varmentamista. (Ries 2011, 64.)

Asiakkaiden ottamista mukaan palveluiden kehittämiseen on luonnollisesti tutkittu. Eräässä tutkimuksessa havaittiin, että asiakkaat tulisi osallistaa kehitystyöhön proaktiivisesti mahdollisimman aikaisessa vaiheessa. Näin asiakkaiden piilevätkin tarpeet voidaan selvittää. (Matthing & Sandén & Evarsson 2004, 494.)

Hyvin menestyvät uudet tuotteet pohjautuvat asiakkaan todellisiin ongelmiin ja tarpeisiin. Tuote ratkaisee sellaisen ongelman tai tarpeen, jota asiakas ei joko kykene tai halua itse ratkaista. (Kinnunen 2004, 42.) Lehtinen ja Niinimäki (2005, 32) kiteyttävät tuotteen olevan se mitä yritys myy tai asiakas haluaa ostaa. Kun yritys on selvittänyt asiakkaalla olevan ongelman tai tarpeen ja on lisäksi päättänyt ratkaista sen, on aika tarkentaa palvelulupaus. Palvelulupaus kiteyttää mikä hyöty tuotteesta on asiakkaalle ja miten yritys lupaa sen toimittaa asiakkaalle. (Jaakkola ym. 2009, 11.) Parantainen kirjoittaa törkeästä lupauksesta. Sen tulee olla helposti mitattavissa, kilpailijoiden lupauksista erottuva. Sen avulla asiakas saadaan uteliaaksi ja se houkuttaa asiakasta ostamaan. (Parantainen 2007, 73.)

2.1.2 Palvelun ominaisuuksien ja sisällön määrittäminen

Kehitettäväksi valitun tai uuden palvelun tuotteistaminen alkaa määrittämällä palvelun keskeiset ominaisuudet. On oleellista tietää, millaista aineetonta tai aineellista hyötyä asiakkaat palvelun avulla tavoittelevat. Tiedon pohjalta suunnitellaan palvelun sisältö ja toteuttaminen niin, että se tuottaa asiakkaalle arvoa. (Jaakkola ym. 2009, 11.) Pelkkä

ominaisuuksien kuvaaminen ei riitä, vaan yrityksen tulee pohtia asiakkaan ostopäätökseen liittyviä kysymyksiä ja etsiä niihin vastauksia (Apunen 2010, 20). Palvelukuvauksen luomista pidetään usein tuotteistamisen kulmakivenä, sillä se auttaa muodostamaan yhteisen merkityksen palvelun eri osapuolille (Tuominen ym. 2015, 14). On tärkeää lähestyä palvelukuvauksen tekemistä asiakasnäkökulmasta, jolloin palvelukuvauksesta saadaan siivotuksi turhat vaiheet (Apunen 2010, 29).

Palvelun sisältö tulee rakentaa vastaamaan asiakkaan tavoittelemaa hyötyä (Tuominen ym. 2015, 17). Asiakkaan todellisten tarpeiden selvittäminen mahdollisimman varhaisessa vaiheessa on suunnittelutyön keskeinen vaihe. Se auttaa varmistamaan palvelun sisällön sopivuuden asiakkaan tarpeisiin. Jos suunnittelutyö perustuu vääriin oletuksiin, saattaa palvelusta tulla asiakkaalle sopimaton. Tällöin tavoiteltu hyöty asiakkaalle jää luomatta ja tuotteella ei ole menestysmahdollisuuksia. (Kinnunen 2004, 42–44.)

Ries (2011, 61) kehottaa vahvistamaan arvohypoteesin eli varmistamaan, että tuote oikeasti tuottaa asiakkaalle arvoa. Kinnunen (2004, 64–70) kutsuu samaa asiaa palvelun tuotantokonseptiksi. Sen avulla tuotteen toimivuutta arvioidaan asiakkaiden kanssa (Kinnunen 2004, 64–70.)

Palvelun sisältö voidaan yleensä jakaa ydinpalveluksi, jota tuetaan tuki- ja lisäpalveluilla. Ydinpalvelulla tarkoitetaan palvelun ominaisuutta, joka vastaa asiakkaan keskeiseen ostotarpeeseen. Lisäpalvelut ovat lähes välttämättömiä ydinpalvelun käytölle, tukipalvelut taas tekevät palvelun käyttämisestä miellyttävämpää. Tätä kokonaisuutta kutsutaan usein palvelupaketiksi. (Kinnunen 2004, 10.)

Palvelupaketin kuvaaminen voi helpottaa erityisesti aineettomien palvelujen myyntiä. Palvelun ostamiseen liittyvä riski tuntuu pienemmältä, kun asiakkaalla on selvä kuva palvelun sisällöstä. Samalla suurien kokonaisuuksien myyminen on helpompaa. Asiakkaan on mahdollista nähdä mistä eri osista palvelukokonaisuus koostuu. Lisäksi asiakas voi itse valita palvelun kanssa ostettavat lisäosat. Tämä mahdollistaa myös selkeämmän hinnoittelun. Lisäosat voi hinnoitella erikseen. (Jaakkola ym. 2009, 11–14; Rissanen 2006, 231–232.)

Palvelun sisällön lisäksi tulee määritellä palvelun tuottaminen ja toteuttaminen. Määrittely kannattaa aloittaa kirjaamalla palvelun toteutusvaiheet ylös riittävän yksityiskohtai-

sesti. Näin selviää ketkä osallistuvat palvelun tuottamiseen missäkin vaiheessa ja millaisella panoksella. Kun tarvittavien resurssien määrä on tiedossa, on palvelun kustannusvaikutuksia helpompi arvioida. (Jaakkola ym. 2009, 15–17; Kinnunen 2004, 64–65.) Määrittelyä helpottaa se, että palvelutuotteen jokaisesta vaiheesta tehdään yksinkertainen lista asiakkaan näkökulmasta (Apunen 2010, 30).

2.1.3 Palvelun vakiointi ja konkretisointi

Palvelun vakioinnin tavoite on sekä suunnitella että mallintaa palvelun vaiheet ja toimintatavat siten, ettei palvelua tai sen osia voi monistaa tai toistaa eri asiakkaille. Näin palvelun tuottaminen on tehokkaampaa, tasalaatuisempaa ja kannattavampaa. Yritys tekee strategisen valinnan sen suhteen, mikä on palvelun vakioitujen ja vakioimattomien osien suhde. Yhdessä ääripäässä on ainutlaatuinen palvelu, jossa ei ole yhtään vakioituja osia. Toinen ääripää on täysin tuotteistettu palvelu, joka toteutuu aina samalla tavalla. (Jaakkola ym. 2009, 19–21.) Apusen (2010, 22) mukaan tuotteistetun palvelun mahdollisimman tehokas monistaminen kuuluu toimitusvaiheeseen.

Suurin osa yrityksistä voi soveltaa tuotteistamista edellä mainittujen ääripäiden väliltä. Palvelun luonne ja yrityksen senhetkinen liiketoimintastrategia ohjaavat, mikä tuotteistamisen aste on missäkin tapauksessa kannattavin. Olennaista on systematisoida palvelu tukemaan asiakkaan kokemaa arvoa ja sopeuttaa vakiointi oikealle tasolle. (Jaakkola ym. 2009, 19.) On tärkeää huomata, että palvelujen perusluonteeseen kuuluu tietynasteinen asiakaskohtainen räätälöitävyys. Tuotteistamisen yhtenä tavoitteena on oikean tasapainon löytäminen vakioinnin ja räätälöinnin välille. (Tuominen ym. 2015, 7.) Oikealla räätälöinnillä yritys voi saavuttaa korkean asiakastyytyväisyyden, hyvän kannattavuuden ja kilpailuedun markkinoilla (Rissanen 2006, 116).

Vakioiduista osista koostuva palvelu saadaan joustavammaksi, jos se jaetaan itsenäisiin moduuleihin, joista asiakkaat voivat kasata tarvitsemansa kokonaisuuden. Modulaarisen palvelun edellytyksenä on, että se koostuu itsenäisistä osista, jotka ovat helposti yhdisteltäviä. (Jaakkola ym. 2009, 19–20.) Palvelun laatuvaihtelut vähenevät, kun palvelu toteutetaan aina samalla ennalta määritellyllä tavalla (Jaakkola ym. 2009, 23).

Tärkeä osa tuotteistamista on konkretisointi. Konkretisoinnilla tarkoitetaan kaikkia niitä keinoja, joilla palvelutuotteen sisällöstä ja sen laadusta on tarkoitus viestiä asiakkaalle

erilaisten näkyvien todisteiden, kuten referenssikuvausten ja tuote-esitteiden avulla. Tavoitteena on luoda asiakkaan ostopäätöksen tueksi mahdollisimman konkreettinen, uskottava, erottumiskykyinen ja helposti ymmärrettävä tuote. (Sipilä 1996, 86; Apunen 2010, 36–37.) Kaikkein tehokkain konkretisoinnin keino asiantuntijapalveluissa on referenssit, asiakkaiden esittelyt ja case-kuvaukset, jotka kertovat hienovaraisesti, miten päästään hyviin tuloksiin (Sipilä 1996, 87).

Tuotteistetulle palvelulle voidaan antaa tuotenimi ja suunnitella oma ulkoasu. Tuotenimen merkitys on itsestään selvä asia, jos tarkoituksena on myydä tuotteistettua palvelua eteenpäin. (Jaakkola ym. 2009, 27.) Tuotteen nimi on olennainen osa tuotteen identiteettiä, joka kertoo, mistä ja kenen tuotteesta on kysymys (Villanen 2016, 145). Hyvä tuotenimi on lyhyt, vapaa rekisteröitäväksi ja soveltuu eri kielialueille (Sipilä 1996, 94).

Standardit, palkinnot ja sertifikaatit viestivät osaamisen tasosta ja palvelun laadusta (Sipilä 1996, 90; Parantainen 2007, 55). Takuun antaminen on vahva tapa viestiä palvelun laadusta. Ostaja arvostaa yritystä, joka ottaa vastuun tuotteensa virheistä. Takuun antaminen laskee asiakkaan kokemaa riskiä. (Parantainen 2007, 56; Jaakkola ym. 2009, 28.)

2.1.4 Seuranta ja mittaaminen

Onnistumisen seuranta ja mittaaminen kuuluvat olennaisesti palvelun kehittämisen ja tuotteistamisen prosessiin. Seuranta on tärkeä osa pitkäjänteistä palveluiden ja liiketoiminnan kehittämistä. Jokaiselle kehitysprojektille täytyy määritellä selkeät tavoitteet ja perusteet, joilla tavoitteiden saavuttamista arvioidaan. Tavoitteiden tulee liittyä selkeästi johonkin kohteeseen ja niiden tulee olla mitattavissa. Selvät arviointiperusteet luovat perustan myös tuotteistamisen tavoitteiden viestinnälle. (Jaakkola ym. 2009, 33.)

Palvelun laatu ja tuottavuus ovat keskeisiä tuotteistamisprojektin seuranta- ja arviointialueita, sillä ne ovat edellytyksiä arvon luomiselle. Tuotteistamisen onnistumista asiakkaiden näkökulmasta voidaan mitata esimerkiksi mittaamalla palvelun laatua ja asiakastyytyväisyyttä. Yksityiskohtaisten seurannan kohteiden ja mittareiden tulee liittyä kiinteästi tuotteistamisprojektille asetettuihin tavoitteisiin, jotta niistä voidaan hyötyä päätöksenteossa. (Jaakkola ym. 2009, 33–34.)

Palvelun laatu on monimutkainen käsite, sillä palvelu on aineeton prosessi. Yleinen näkemys on kuitenkin se, että palvelun laatu on sitä, miten asiakkaat sen kokevat. Jos

palvelun laatu vastaa asiakkaan odotuksia, on laatu hyvää. Palvelun laatu syntyy saavuttamalla tai ylittämällä asiakkaan odotukset. (Jaakkola ym. 2009, 34.) Palvelun laadun mittaamiseen, vain odotusten ja kokemusten erona, on kohdistettu kritiikkiä. On paradoksaalista ajatella palvelun laadun mittaamista odotusten ja kokemusten erona tilanteessa, jossa asiakkaalla on alhaiset odotukset palvelun laadun suhteen. Tällöin ylittämällä asiakkaan alhaiset odotukset rimaa hipoen, voitaisiin kuitenkin todeta palvelun laadun olleen hyvää. Näinhän asia ei voi olla. (Kinnunen 2004, 19.)

Tuottavuudella tarkoitetaan yrityksen sisäistä palveluntuottamisprosessin suorituskykyä ja se mittaa tuotosten ja käytettyjen panostusten välistä suhdetta. Palvelun tuottavuutta on usein haastavaa mitata, sillä käytettyjä panostuksia on usein hankala eritellä. Tuotteistamisen myötä mittaaminen on helpompaa, koska yrityksellä on tarkempi näkemys siitä, mitä resursseja ja kuinka paljon niitä tarvitaan tietyn palvelun tuottamiseksi. (Jaakkola ym. 2009, 36.)

Tuotteistamisprosessi ei suinkaan pääty projektin onnistumisen mittaamiseen, vaan kehitetty palvelu siirtyy osaksi yrityksen sen hetkistä palvelutarjoomaa. Yrityksen tulisikin arvioida palvelutarjoomaa kriittisesti säännöllisesti, myös varsinaisten kehityshankkeiden välillä. (Jaakkola ym. 2009, 39.)

2.2 Tuotteistamisen hyödyt ja haasteet

Tuotteistamisen hyötyihin voidaan laskea muun muassa tasalaatuisempi palvelu, toistettava palvelu, myynnin ja markkinoinnin helpottuminen sekä palvelun jatkokehittämisen helpottuminen. Palvelun vakioiminen mahdollistaa henkilöriippumattoman ja tasalaatuisen palvelun. Kun yrityksen sisällä on yhteinen ymmärrys vakioidun palvelun sisällöstä, on siitä helpompi viestiä yhdenmukaisesti. Tuotteistamisen seurauksena luotu markkinointimateriaali ja palvelukuvaukset helpottavat tuotteen esittelyä asiakkaille. Lisäksi tuotteistamisen myötä yritykselle kehittyy parempi käsitys palvelun roolista ja siitä, miten palvelu linkittyy yrityksen palvelutarjoomaan ja strategiaan. (Tuominen ym. 2015, 7.) Tuotteistaminen auttaa usein myös yritystä kasvuun laajentamalla asiakassegmenttiä ja lisäämällä markkinaosuutta (Lehtinen & Niinimäki 2005, 27).

Monen yrityksen haasteena jatkuvasti kiristyvässä kilpailussa on tuottavuuden ja laadun nostaminen samalla, kun yrityksen tulee kehittää lyhyen ajan tulosta ja pitkän ajan kannattavuutta. Tuotteistaminen on osaamisen kehittämisen ohella se keino, jolla yritys voi

ratkaista laadun ja tuottavuuden sekä lyhyen ja pitkän aikavälin tavoitteiden ristiriitaisen yhtälön. Tuotteistamisella voidaan parantaa tehokkuutta ja laatua, kun toiminnasta tulee systematisoidumpaa ja suunnitelmallisempaa analysoimalla ja selkeyttämällä työvaiheita ja täsmentämällä tavoitteita. (Sipilä 1996, 18–19.)

Koska tuotteistaminen pakottaa yrityksen selkiinnyttämään liiketoimintastrategiaansa ja toimintaprosessejaan, on sen myös päätettävä mitä osaamista tarvitaan ja mihin tuotteisiin keskitytään. Tämän johdosta päätöksenteko ja vastuualueet selkiintyvät, mikä helpottaa johtamista ja toiminnan hallintaa. (Sipilä 1996, 21.)

On tärkeä tiedostaa, että tuotteistamiseen liittyy myös haasteita ja riskejä. Suureen osaan niistä on mahdollista vastata osallistamalla henkilöstö ja asiakkaat tuotteistamisessa. Haasteisiin lukeutuvat muun muassa asiakasnäkökulman hukkuminen ja tuotteistamisen kokeminen uhkana. Jos henkilöstö kokee tuotteistamisen olevan uhaksi omalle osaamiselleen, eivät he ole valmiita jakamaan parhaita toimintatapojaan. Jos taas tuotteistamisen aikana syntyvä palvelu on liian jäykkä, on vaarana asiantuntijoiden motivaation mureneminen, kun he eivät enää voi räätälöidä palvelua asiakaskohtaisesti. Samalla vaarana on, että uusia ideoita ei ole mahdollista hyödyntää palvelun kehittämiseksi. (Tuominen ym. 2015, 7–8.)

Henkilöstön osallistamisessa on tärkeää huolehtia, että osallistuvan henkilöstön henkilökohtaiset tavoitteet ovat linjassa tuotteistamisen tavoitteiden kanssa ja että henkilöstön keskinäinen luottamus on vahvalla pohjalla. Jos tavoitteet eivät kohtaa ja keskinäinen luottamus ei ole kunnossa, henkilöstö ei ole valmis jakamaan osaamistaan ja sitoutumaan tuotteistamisprosessiin. (Valtakoski & Järvi 2016, 383.)

Tehokas palvelujen tuotteistaminen merkitsee usein muutosta organisaation toimintatapoihin. Se tuo haasteita uuden toimintatavan juurruttamiseen organisaatioon ja henkilöstön sitouttamiseen muutokseen. Koska systematisoinnin avulla siirretään vahvasti henkilöitynyttä osaamispääomaa koko organisaation yhteiseksi omaisuudeksi, vaatii muutos niin sisäistä markkinointia kuin aikaa. (Jaakkola ym. 2009, 39.) Sisäisen markkinoinnin avulla henkilöstöä tuetaan ja ohjataan luottamaan tuotteisiin ja tavoitteisiin (Lehtinen & Niinimäki 2005, 16).

2.3 Hinnoittelu

Hinta on palvelun voimakkain ominaisuus, ja se viestii palvelun laadusta (Rissanen 2006, 230). Selkeä hinnoittelu konkretisoi palvelun asiakkaalle, kun hänelle on mahdollista kertoa, mitä asiakas tulee saamaan ja mitä se tulee maksamaan. Hinnoittelun ei tarvitse olla suoraviivaista kaavan soveltamista. Yhtenä perusteena tulee kuitenkin olla tarkka laskelma kustannuksista, joita palvelun tuottamisesta aiheutuu. (Jaakkola ym. 2009, 29.) Hinnoittelussa tulee ottaa huomioon myös markkinatilanne, sillä hintoihin vaikuttaa vahvasti myös kilpailu sekä vallitseva kilpailutilanne (Villanen 2016, 171).

Hinnoittelun ymmärtäminen on kriittisen tärkeää yrityksen kannattavuuden kannalta (Villanen 2016, 171). Palvelun tuottamisen kustannukset ovat hinnoittelun perusta siinäkin tapauksessa, että palvelun hinnoittelu ei perustuisikaan pelkästään kustannuksiin. Markkinatilanne vaikuttaa hintaan palvelun kysynnän ja menekin kautta. Asiakkaiden hintaodotusten lisäksi palvelun hintaan vaikuttaa palvelun asiakkaalle tuoma lisäarvo. (Jaakkola ym. 2009, 29.) Hinnoittelussa on tärkeää pyrkiä löytämään sopiva tasapaino, jotta yritys kykenee ennakoimaan kysyntää ja synnyttää tuotteilleen riittävän katteen (Villanen 2016, 172).

Useimmissa tapauksissa sekä markkinat että tuotantokustannukset vaikuttavat palvelun hinnoitteluun. Todelliset tuotantokustannukset määrittävät käytännössä palvelun hinnalle alarajan. Markkinat ja kysyntä määrittävät hinnalle ylärajan. Mitä ainutlaatuisempaa palvelua tarjotaan, sitä vähemmän on merkitystä kilpailijoiden hinnoilla. (Jaakkola ym. 2009, 29; Villanen 2016, 172.)

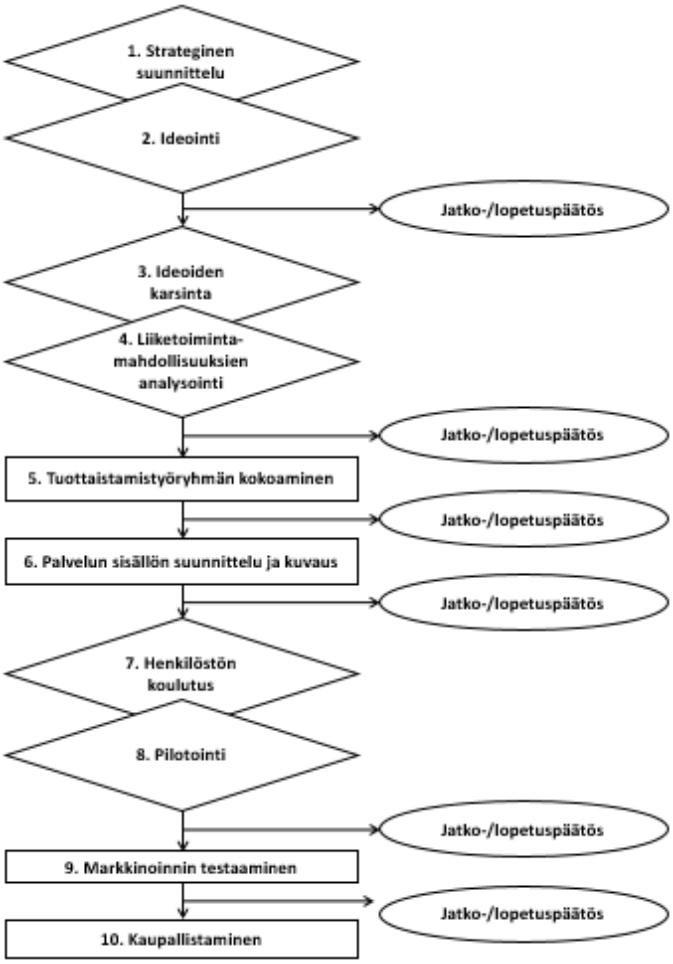
Hinnoittelutapoja on runsaasti, eikä yhtä oikeaa tapaa ole olemassa (Villanen 2016, 172). Tavat voidaan jakaa esimerkiksi tuotosperusteiseen, resurssipohjaiseen, hyöty- ja arvoperusteiseen sekä käyttöoikeusperusteiseen hinnoitteluun. Tuotosperusteisessa hinnoittelussa asiakas maksaa palvelusta kiinteän hinnan. Resurssipohjaisessa hinnoittelussa hinta perustuu käytettyyn aikaan tai varattuun kapasiteettiin. Hyöty- ja arvoperusteinen hinnoittelu perustuu asiakkaan saamaan hyötyyn. Käyttöoikeusperusteinen hinnoittelu perustuu käyttöoikeuteen. (Jaakkola ym. 2009, 30; Rissanen 2006, 230.)

Hinnoittelun perusteita ja hinnoittelutapoja valitessa tulee yrityksen miettiä palvelun hintaa asiakkaan näkökulmasta (Jaakkola ym. 2009, 30). Asiakasta ei kiinnosta, kuinka pal-

jon palvelu maksaa sen tuottajalle, eikä asiakkaalla yleensä ole aavistustakaan kustannuksista. Tämän sijaan asiakas vertaa palvelun hintaa suhteessa saamaansa hyötyyn ja markkinoiden kilpaileviin palveluihin. Koska tuotteistaminen lisää vertailtavuutta, tulee asiakkaasta hintatietoisempi. Yritys voi pyrkiä vaikeuttamaan vertailua tarjoamalla niin ainutlaatuista palvelua, ettei sitä voi suoraan verrata muihin tuotteisiin. (Apunen 2010, 38–39.) Hinnan määrittelemiseen kannattaa käyttää aikaa, jotta sen saa asetettua oikealle tasolle. Asetettua hintaa on vaikea muuttaa heti tuotteen lanseeraamisen jälkeen. (Villanen 2016, 171.)

2.4 Asiakaslähtöisen tuotteistamisprosessin malli

Kuviossa 1 on esitetty asiakaslähtöisen tuotteistamisprosessin malli. Se perustuu Alamin ja Perryn (2010, 525) luomaan asiakaslähtöiseen uuden palvelun kehittämisen malliin.



Kuvio 1. Asiakaslähtöisen tuotteistamisprosessin malli (mukaillen Alam & Perry 2010, 525).

Tämä opinnäytetyö noudattaa kuviossa 1 esitettyä tuotteistamisprosessia soveltuvin osin. Opinnäytetyö keskittyy edellä mainitun tuotteistamisprosessin vaiheeseen 6, jonka yksi osa-alue on palvelun sisällön tarkentaminen vastaamaan asiakkaiden tarpeisiin.

3 Identiteetin- ja pääsynhallinta

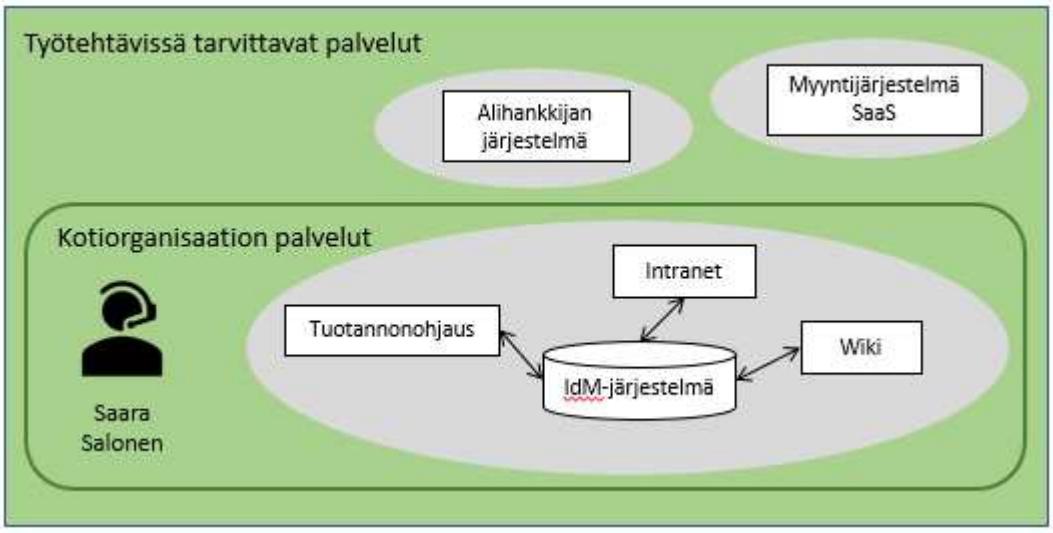
Identiteetin- ja pääsynhallinnan käsite (Identity And Access Management, IAM) koostuu identiteetinhallinta-käsitteestä (Identity Management, IdM) ja pääsynhallinta-käsitteestä (Access Management, AM). Identiteetinhallinnalla tarkoitetaan prosessia, jonka avulla kohteet esitetään digitaalisina identiteetteinä eri tietojärjestelmissä. Tämän lisäksi siihen liittyy toimintakäytäntöjä, joilla tietojärjestelmissä olevia tietoja ylläpidetään. Identiteetinhallinnan kanssa käytetään usein pääsynhallinta-käsitettä, jolla tarkoitetaan sitä toimintoa, jossa tapahtuu käyttäjän tunnistus ja tunnistukseen perustuen tehdään päätös, onko käyttäjällä pääsy tietojärjestelmään. (Linden 2015, 10–11.) Identiteetin- ja pääsynhallinnan käsitteestä käytetään myös nimitystä käyttövaltuushallinta (Kuntaliitto 2013a, 6).

Kun identiteetin- ja pääsynhallintaa toimitetaan palveluna, nimitetään sitä yleensä IDaaS-palveluksi (Identity and Access Management as a Service). Tutkimuslaitos Gartnerin ennusteen mukaan vuoteen 2020 mennessä 40 prosenttia identiteetin- ja pääsynhallinnan tuotteista myydään IDaaS-mallilla (Kreizman & Wynne 2016).

Tässä opinnäytetyössä identiteetin- ja pääsynhallinnan käsitteeseen tutustutaan pääasiassa organisaatiokeskeisesti. Itse käsite alkoi muodostua vuosituhannen vaihteessa, kun käyttäjän tunnistusta vaativat palvelut alkoivat yleistyä. Varsinkin isommissa organisaatioissa käyttäjätunnusten avaaminen, sulkeminen ja unohtuneet salasanat työllistivät turhan paljon IT-tukea. Pian havaittiin myös muita tietoturvaongelmia, kuten sulkematta jääneet käyttäjätunnukset ja heikkoudet salasanatunnistuksessa. (Linden 2015, 4.)

Tietotekniikka-alalla alettiinkin kehittää tuotteita, joiden avulla käyttäjätunnuksia, käyttövaltuuksia ja salasanoja voitiin hallinnoida aiempaa keskitetymmin. Identiteetin- ja pääsynhallinnan tuoteperhe alkoi vähitellen muotoutua. Tuotteiden avulla voitiin toteuttaa järjestelyjä, joissa käyttäjällä on organisaatiossa yksi identiteetti. Identiteettiin kytketyllä käyttäjätunnuksella käyttäjä pääsee kirjautumaan ainakin kaikkiin keskeisimpiin organisaation sisäisiin palveluihin, joihin hänelle on myönnetty käyttövaltuus. (Linden 2015, 4.)

Järjestely on havainnollistettu kuviossa 2, jossa harmaat alueet kuvastavat yhden identiteetin kattavuutta.



Kuvio 2. Keskitetty identiteetinhallinta organisaation sisällä (mukaillen Linden 2015, 4).

Ennen kuin opinnäytetyö etenee organisaatioiden keskitettyyn identiteetinhallintaan, tutustutaan käsitteistöön, joiden ymmärtäminen auttaa kokonaisuuden hahmottamisessa. Aloitetaan identiteetin- ja pääsynhallinnan kehittämisen hyödyistä. Tämän jälkeen jatketaan identiteetin käsitteeseen, identiteetin todentamiseen ja käyttövaltuuksien hallintaan. Jäljitettävyyden ja raportoinnin kautta palataan identiteetinhallintaan organisaatioissa. Lopuksi tutustutaan federoituun identiteetinhallintaan, joka mahdollistaa organisaation ulkopuolisten järjestelmien käytön samalla identiteetillä.

3.1 Hyödyt

Identiteetin- ja pääsynhallinnan kehittämisen kautta organisaation on mahdollista saavuttaa erilaisia hyötyjä (Linden 2015, 6). Identiteetinhallinnassa suurena ongelmana on, että käyttäjän käyttövaltuuksia ei usein muisteta poistaa, kun perusteet käyttövaltuuksille lakkaavat olemasta. Tyypillisesti näin käy työpaikan vaihdon yhteydessä, kun työntekijän käyttäjätunnuksia eri järjestelmissä ei muisteta sulkea. (F5 2016.) Jos työntekijällä on vain yksi keskitetysti ylläpidetty käyttäjätunnus, jonka sulkeminen katkaisee kaikki käyttövaltuudet kaikissa palveluissa, saadaan työntekijän kirjautuminen eri järjestelmiin päätettyä kerralla. (Linden 2015, 6).

Jos käyttäjällä on jokaisessa palvelussa oma käyttäjätunnus, kasvaa tarvittavien käyttäjätunnus-salasana-parien määrä liian suureksi muistettavaksi. Tämä johtaa siihen, että käyttäjä joutuu lopulta kirjoittamaan käyttäjätunnukset ja salasanat johonkin talteen. (Linden 2015, 6–7.) Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän teettämän kyselyn mukaan 53,5 prosenttia vastaajista ilmoitti tarvitsevansa kuutta tai useampaa käyttäjätunnusta/salasanaa työtehtäviensä hoitamiseksi. Jopa 9,2 prosenttia vastaajista ilmoitti määräksi 16 tai useampi. (Valtiovarainministeriö 2016b, 49–50.)

Identiteetin- ja pääsynhallinnan kehittämisellä pyritään usein mahdollistamaan useampaan palveluun kirjautuminen samalla käyttäjätunnuksella ja salasanalla. Tämä luo samalla riskin, sillä yksi paljastunut salasana voi mahdollistaa useiden palveluiden väärinkäytöksen. Jos käyttäjällä kuitenkin on vain yksi identiteetti, jota ylläpidetään keskitetysti, on luotu edellytykset vahvalle tunnistautumiselle. (Linden 2015, 7.)

Organisaatiot pyrkivät toimimaan tehokkaasti karsimalla ja automatisoimalla turhia työvaiheita. Työntekijöille tehokkuus näkyy esimerkiksi työajan säästönä. Jos käyttäjän tulee muistaa vain muutama käyttäjätunnus/salasana-pari, vähenee unohtuneiden salasanojen palauttamista tai uusimista koskevat tukipyynnöt, jolloin IT-tuen työkuorma vähenee. (Linden 2015, 7; F5 2016.)

Usein käyttäjillä on käyttöoikeus useaan eri tietojärjestelmään. Jos jokaisessa tietojärjestelmässä erikseen perustetaan, ylläpidetään ja suljetaan saman käyttäjän erillisiä tunnuksia, tehdään organisaatiossa moneen kertaan samaa päällekkäistä työtä. (F5 2016.) Samalla riski tietojen eheyden osalta kasvaa, sillä muuttuvia tietoja ei välttämättä muisteta viedä kaikkiin tietojärjestelmiin. Keskitetyllä hallinnalla vähennetään samojen tietojen moninkertaista syöttämistä sekä parannetaan tiedon laatua. (Linden 2015, 7.)

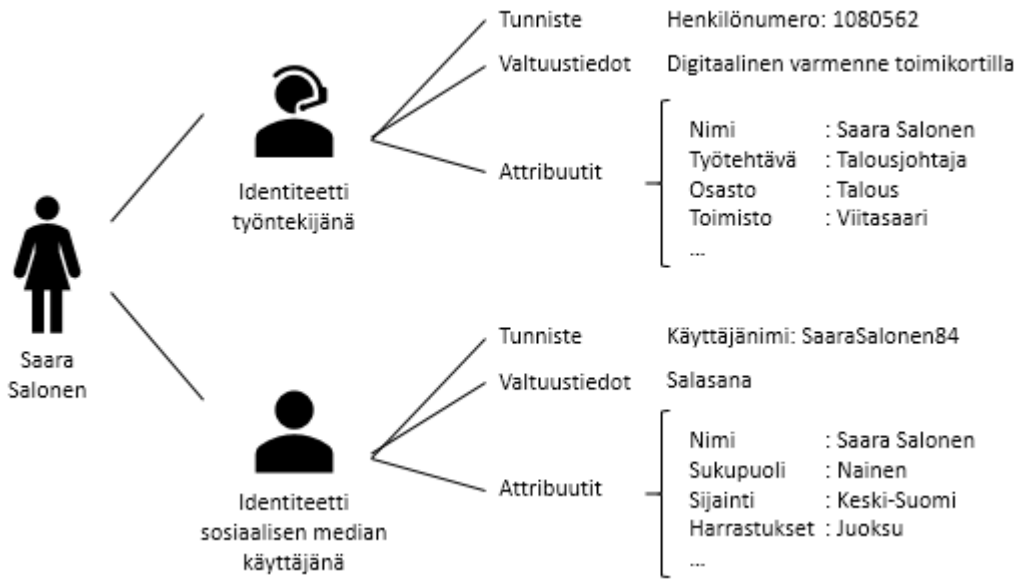
Keskitetyn hallinnan ja automatisoinnin kautta myös tietoturva paranee, sillä inhimillisiä virheitä saadaan karsittua tietojen syöttämisessä ja poistamisessa. Lisäksi keskitetty hallinta mahdollistaa merkittäviä säästöjä, tekemällä käyttöoikeuksien hallinnasta tehokkaampaa. (Valtori 2017.)

Tietoturvan parantumisen ja toiminnan tehostumisen lisäksi identiteetin- ja pääsynhallinnan kehittäminen voi mahdollista organisaation toiminnan uudelleenjärjestelyn tai uusien liiketoimintamallien kehittämisen. Tietotekniikan käytön lisääntyessä myös itsepalvelumallia tukevat tietojärjestelmät lisääntyvät. Jos kaikkien palveluiden käyttöön tarvitaan

yhtä käyttäjätunnus/salasana-paria, itsepalveluperiaatteen käyttöönotto on mahdollista myös sellaisten palveluiden osalta, joita käytetään harvemmin. (Linden 2015, 8.)

3.2 Identiteetti

Tietotekniikassa sähköisellä identiteetillä tarkoitetaan kohteen kuvailevien ominaisuuksien joukkoa eli attribuuttien kokoelmaa, joka on talletettu johonkin tietojärjestelmään ja jonka avulla kohde voidaan tunnistaa. (Valtiovarainministeriö 2006, 43.) Kohteet ovat yleensä ihmisiä, joita voidaan kuvailla esimerkiksi seuraaville attribuuteilla: koko nimi, kotipaikka ja syntymäpaikka (Bertino & Takahashi 2011, 22). Lisäksi attribuuttina voi toimia esimerkiksi sähköpostiosoite, käyttäjätunnus sekä valtuus jonkun palvelun käyttämiseksi. Käyttötilanteesta riippuu, mitä attribuutteja milloinkin on tarpeellista liittää identiteettiin. (Linden 2015, 10–11.) Kuviossa 3 on esitetty Saara, jolla on kaksi erillistä identiteettiä, yksi työntekijänä ja toinen sosiaalisen median käyttäjänä.



Kuvio 3. Identiteetteihin liitetyt attribuutit (mukaillen Bertino & Takahashi 2011, 24).

Käyttäjää kuvaavien ominaisuuksien eli attribuuttien joukosta kannattaa erikseen huomioida yksilöivät tunnisteet (Unique identifier). Niitä käytetään, jotta käyttäjät voidaan erottaa toisistaan jossakin nimiavaruudessa. Esimerkiksi organisaation eri käyttäjillä tulee olla yksilöllinen käyttäjätunnus ja sähköpostiosoite. (Linden 2015, 12.) Kuviossa 3 työntekijän yksilöivä tunniste voisi olla työpaikan henkilönumero ja sosiaalisen median käyttäjänä yksilöivä tunniste voisi olla käyttäjänimi.

Yksilöivät tunnisteet ovat identiteetinhallinnassa hyvin keskeisessä asemassa ja kaikilla käyttäjillä tuleekin olla yksilöivä tunniste kaikissa käyttövaltuushallintoon liittyvissä tietovarastoissa (Valtiovarainministeriö 2006, 28). Koska yksilöivällä tunnisteella tulee voida viitata yksiselitteisesti tiettyyn käyttäjään, ei sen arvoa voi jättää yhdenkään käyttäjän osalta tyhjäksi (Linden 2015, 12–13).

3.3 Identiteetin todentaminen eli autentikointi

Identiteetin todentamisella tarkoitetaan identiteetin varmentamista. Tietojärjestelmä varmistaa, että sisään kirjautuu se henkilö, joka hän väittää olevansa. (Pfleeger & Pfleeger & Margulies 2015a.) Samalla tietojärjestelmä varmistaa, että järjestelmään luotu tietty identiteetti kuuluu kyseiselle henkilölle. Voidaan todeta, että autentikointia ei voi tapahtua, jos käyttäjällä ei ole järjestelmässä olemassa ainakin jonkinlaista identiteettiä. Kytkös on yleensä voimassa istunnon ajan, joka päättyy, kun käyttäjä kirjautuu ulos. (Linden 2015, 16.)

Identiteetin todentamiseksi on useita erilaisia menetelmiä, jotka eroavat luotettavuudeltaan. Ne jaetaan yleensä kolmeen eri ryhmään:

1. Jotain, mitä henkilö tietää (esimerkiksi pääsykoodi, salasana tai salainen kättely)
2. Jotain, mitä henkilöllä on hallussa (esimerkiksi pankki- tai toimikortti)
3. Jotain, mitä henkilö on tai miten henkilö käyttäytyy (biometrinen tunnistaminen, esimerkiksi kasvot tai sormenjäljet). (Pfleeger ym. 2015b.)

Jos vähintään kaksi tekijää yllämainituista ryhmistä on yhtä aikaa läsnä, pidetään identiteetin todentamista usein vahvana. Esimerkiksi pankkiautomaatilla asioidessa tarvitaan sekä pankkikortti että PIN-koodi. (Valtiovarainministeriö 2008, 124.) Käyttäjien luotettava tunnistaminen on sitä tärkeämpää mitä hienojakoisempia käyttövaltuuksia ja suojaustarpeita tietojärjestelmässä on (Valtiovarainministeriö 2006, 27).

Kertakirjautumisen (single sign-on, SSO) käsite esiintyy usein identiteetin- ja pääsynhallinnan yhteydessä (Linden 2015, 29). Kertakirjautuminen on pääsynvalvonnan toteutustapa, jossa käyttäjän tarvitsee tunnistautua vain kerran. Tämän jälkeen hän pääsee kaikkiin saman pääsynvalvonnan piirissä oleviin palveluihin käyttövaltuuksiensa puitteissa ilman uutta tunnistautumista. (Valtiovarainministeriö 2008, 49.)

3.4 Käyttövaltuuksien hallinta eli auktorisointi

Tietojärjestelmien käyttäjät haluavat usein luoda ja lukea tiedostoja. Käyttäjän tunnistamisen jälkeen tuleekin selvittää, onko käyttäjällä valtuudet suorittaa pyydetty toiminto. Puhutaan pääsynvalvontapäätöksestä, joka käyttäjän tunnistuksen kanssa yhdessä muodostavat toimintosarjan, jota kutsutaan pääsynvalvonnaksi. (Bertino & Takahashi 2011, 153–154.) Pääsynvalvonta onkin hyvin keskeinen osa-alue pääsynhallintaa, johon sisältyy myös käyttövaltuuksien hallinta (Linden 2015, 31).

Usein pääsynvalvontapäätös ja sen edellyttämä logiikka sisältyvät palveluun, johon ollaan kirjautumassa. Se voidaan kuitenkin eriyttää omaksi palveluksikin. Pääsynvalvonnan lähtökohtana on, että käyttäjä on jo tunnistettu. Usein käyttäjän tunnistus on suoritettu ”riittävän luotettavasti”, mutta joskus suojattavat kohteet tai toiminnot voivat vaatia vahvempaa tunnistusta. Tunnistuksen vahvuutta voidaan käyttää yhtenä pääsynvalvontapäätökseen vaikuttavana käyttäjän attribuuttina. (Linden 2015, 31–32.)

Pääsynvalvontamatriisi on klassinen keino kuvata käyttäjällä olevat käyttövaltuudet suojattavana olevaan kohteeseen. Käyttäjät on esitetty riveillä ja suojattavat kohteet matriisin sarakkeissa. Soluihin kirjataan käyttäjille sallitut toiminnot. (Pfleeger ym. 2015g.) Esimerkki pääsynvalvontamatriisista on esitetty taulukossa 1.

Taulukko 1. Esimerkki pääsynvalvontamatriisista (mukaillen Linden 2015, 32).

	/home/mikko/docs	/topsecret	/tmp/foo
Mikko	read, write	-	read
Maija	read	-	read, write

Käyttäjien ja suojattavien kohteiden määrän kasvaessa, pääsynvalvontamatriisin ylläpitämisestä tulee mahdotonta (Valtiovarainministeriö 2006, 18). Tämän vuoksi on kehitetty muita pääsynhallintamalleja kuten rooliin perustuva pääsynvalvonta ja attribuuttiin perustuva pääsynvalvonta (Linden 2015, 32–35).

Käyttövaltuuksia määriteltäessä ei ole käytännöllistä tarkastella käyttäjiä yksilötasolla, vaan tulee pyrkiä löytämään käyttäjäryhmiä, joilla on samankaltaiset tarpeet (Valtiovarainministeriö 2006, 17). Rooliin perustuvassa pääsynvalvonnassa (role-based access control, RBAC) on luotu roolin käsite. Käyttäjälle annetaan hänen tarpeitaan kuvaavia

rooleja, joille käyttövaltuudet annetaan. (Pfleeger ym. 2015d.) Tarkoituksenmukaisten roolien tunnistaminen on rooliin perustuvan käyttövaltuushallinnan suunnittelun keskeinen vaihe (Linden 2015, 33; Pfleeger ym. 2015c). Rooli voi olla esimerkiksi työrooli tai järjestelmärooli kohdejärjestelmässä tai muussa järjestelmässä (Mäntykangas 2017).

Rooliin perustuvassa pääsynhallinnassa roolit voidaan rakentaa hierarkkisesti, jolloin roolit perivät oikeuksia toisilta rooleilta (Kuhn & Coyne & Weil 2010, 1). Rooleissa ja niiden jäsenyyksissä tapahtuvat muutokset ja niiden hallinta ovat kriittisiä osia käyttövaltuuksien hallintaa. On tärkeää, että tarpeettomaksi käyneet käyttövaltuudet poistetaan välittämättömästi. (Valtiovarainministeriö 2006, 19–20.)

Organisaatioilla on kuitenkin tullut esille tarve päästä rooleihin perustuvan pääsynhallinnan rajojen yli. On tullut tarve sisällyttää pääsynhallintaan erilaisia attribuutteja, kuten kellonaika ja käyttäjän paikkatieto. Tähän tarpeeseen vastaa attribuuttiin perustuva pääsynvalvonta (attribute-based access control, ABAC). (Coyne & Weil, 2013, 14.) Se perustuu roolin sijaan mihin tahansa käyttäjän, ympäristön, operaation tai palvelun attribuuttiin (Linden 2016, 35). Attribuuttiin perustuva pääsynvalvonta on joustavampi ja helpompi määritellä eikä se vaadi erilaisia rooleja käyttäjän eri attribuuteille. Joustavuuden vastapainona kaikkien erilaisten mahdollisten attribuuttiyhdistelmien tarkistaminen on huomattavasti monimutkaisempaa. (Kuhn ym. 2010, 79–80).

Käyttövaltuuksien hallinta perustuu pienimmän käyttövaltuuden periaatteeseen, joka on yksi tietoturvallisuuden keskeisiä periaatteita. Käyttäjällä tulee periaatteen mukaan olla käytössään mahdollisimman alhaiset käyttövaltuudet työtehtäviensä hoitamiseksi. (Pfleeger ym. 2015c.) Muutenhan kaikki käyttäjät voisivat aina saada kaikki valtuudet eikä käyttövaltuuksien hallinnalle olisi tarvetta. Pienimmän käyttövaltuuden periaatteeseen kuuluu lisäksi se, että laajoja käyttöoikeuksia käytetään vain kyseisiä käyttöoikeuksia vaativiin toimenpiteisiin. Näin pyritään ehkäisemään inhimillisiä virheitä ja väärinkäytöksiä. (Linden 2015, 36.)

Ponemon Instituten (2017, 4) tutkimuksen mukaan lähes puolet yritysten kokemista tietomurroista on tehty sisäpiirin tai rikollisten toimesta. Verizonin (2017, 3) raportti paljastaa, että tietomurroista 14 prosenttia tehtiin väärinkäyttämällä yrityksen sisäisiä tunnuksia.

Erilaisten ylläpitotunnusten väärinkäytön riskiä voidaan pienentää PAM-järjestelmällä (Privileged Account Management). Järjestelmän avulla hallinnoidaan ylläpitotunnuksia ja sen kautta käyttäjä saa käyttöön tarvitsemansa ylläpitotunnuksen. (Hintsanen 2014.) Päätarkoitus on tunnistaa henkilö ylläpitäjäidentiteetin takaa, sillä ylläpitäjät käyttävät usein samaa ylläpitotunnusta. Näin ylläpitäjä saadaan yhdistettyä todelliseen henkilöön. (Mäntykangas 2018c.) Tunnistautuminen voidaan tarvittaessa suojata vahvalla tunnistautumisella ja toteuttaa siten, ettei käyttäjä saa tietoonsa järjestelmän ylläpitoon tarvittavaa salasanaa (Hintsanen 2014). PAM-järjestelmissä usein myös tallennetaan laajojen käyttöoikeuksien käyttöön liittyvät istunnot (Wagner 2015).

Inhimillisiä virheitä ja väärinkäytöksiä pyritään estämään myös vaarallisten työtehtävien eriyttämisellä (Linden 2015, 37). Rooleja tai niiden yhdistelmiä, joihin sisältyy riski vaarallisista käyttövaltuuksista, tulee välttää. Jos niitä kuitenkin on pakko myöntää, tulee niiden käyttöä valvoa normaalia tarkemmin. (Valtiovarainministeriö 2006, 20.) Hyvä identiteetinhallintajärjestelmä osaa automaattisesti raportoida sekä tarvittaessa estää vaarallisten työtehtävien yhdistelmän (Mäntykangas 2018c).

3.5 Jäljitettävyys ja raportointi

Jäljitettävyys ja raportointi ovat yleensä käyttäjälle näkymättömiä toimintoja. Ne ovat kuitenkin tärkeässä roolissa identiteetin- ja pääsynhallinnan tietoturvaa täydentävinä kontrolleina. (Linden 2015, 39.)

Jäljitettävyydellä tarkoitetaan luotettavan kirjausketjun luomista tapahtumista, jotka liittyvät identiteetin- ja pääsyhallintaan. Kirjausketjun tarkoituksena on voida tarvittaessa osoittaa, kuka teki tietyn toimenpiteen sekä mihin kyseisen toimenpiteen valtuus perustui. Kirjausketjua on mahdollista käyttää tarpeen mukaan todistusaineistonakin. (Linden 2015, 39.) Käyttövaltuushallinnon hyviin käytäntöihin kuuluu, että käyttövaltuuksiin ja niiden määrityksiin tehdyt muutokset ovat jäljitettävissä siten, että kaikki muutostapahtumiin osalliset käyvät selville (Valtiovarainministeriö 2006, 26).

Keskeinen rooli jäljitettävyyden toteuttamisessa on lokitiedostoilla. Niitä kerätään muun muassa käyttäjien tunnistamiseen, käyttäjien käyttövaltuuksien myöntämiseen, muutoksiin ja käyttämiseen liittyen. (Valtiovarainministeriö 2006, 26.) Lokitietojen kerääminen sekä lokitietojen eheys tulee varmistaa yrityksen muun lokitietojen hallinnan yhteydessä

(Linden 2015, 39). Lokitietojen käsittelyä säätävät muun muassa henkilötietolaki, julkisuuslaki, laki yksityisyyden suojasta työelämässä ja tietoyhteiskuntakaari. Lainsäädäntö rajoittaa lokitietojen käsittelyä erityisesti tapauksissa, joissa lokeihin tallentuu joko tunnistamistietoja tai henkilötietoja. (Valtiovarainministeriö 2009, 20–21.)

Raportoinnin tehtävänä on täydentää jäljitettävyyttä. Raportointivälineiden avulla on mahdollista tutkia järjestelmässä olevien identiteettien ja käyttövaltuuksien tila. (Linden 2015, 39.) Lisäksi ne mahdollistavat, vaikka yksittäisen identiteetin käytön seurannan (Valtiovarainministeriö 2006, 26–27). Järjestelmän tulee mahdollistaa ajantasaiset raportit käyttäjistä, rooleista, käyttövaltuuksista ja niiden erilaisista yhdistelmistä (Valtiovarainministeriö 2006, 21). Raportoinnin kautta tulee saada vastaukset seuraaviin kysymyksiin: Kenelle on myönnetty oikeus mihinkin järjestelmään ja milloin? Kuka on käyttänyt tiettyä järjestelmää ja milloin? (Kreizman & Wynne 2016.)

Siinä missä IAM-tuotteet keskittyvät identiteetin- ja pääsynhallintaan, IAG- (Identity and Access Governance) ja IGA-tuotteiden (Identity Governance and Administration) tarkoituksena on tarjota strategisempi hallintotaso identiteetin- ja pääsynhallintaan. Tuotteet tarjoavat tietojen näyttämiseen ja hallinnointiin käyttöliittymän, erilaisia näkymiä ja suorituskykymittareita. Niiden avulla yritykset pyrkivät varmistamaan ja näyttämään toteen, että he noudattavat sääntöjä ja asetuksia. Lisäksi tuotteiden avulla saadaan vastauksia muun muassa kysymyksiin: Missä piilee suurimmat riskit identiteettien ja käyttäjätilien osalta? Millä perusteilla käyttövaltuudet myönnetään? Miten usein tietojen ja käyttöoikeuksien oikeellisuus tarkistetaan ja kenen toimesta? (Flynn 2012; Iverson 2015.) Tämän lisäksi tuotteilla voidaan tarkistaa myös ne järjestelmät, jotka eivät ole kiinni identiteetinhallintajärjestelmässä. Tai jos ovat, niin voidaan tarkistaa, että toimiiko identiteetinhallintajärjestelmä oikein. (Mäntykangas 2018b.) Gartnerin tutkimuslaitos arvioi, että vuoteen 2019 mennessä yli 30 prosenttia uusista IGA-tuotteiden käyttöönotoista ostetaan palveluna (Gaehtgens & Carepenter & Iverson & Kampman 2017).

Eri järjestelmistä ja laitteista kerätyistä lokitiedostoista muodostuu helposti valtava määrä tietoa. Organisaatio voi SIEM-järjestelmän (Security Information and Event Management) avulla hallinnoida tietoturvatapahtumia keskitetysti. Se yhdistää lokienkeräämisen ja raportoinnin reaaliaikaiseen tapahtumien analysointiin sekä havaintojen perusteella tehtäviin automaattisiin toimintoihin, kuten hälytyksiin. (Edwards 2017, 2.) Usein SIEM-järjestelmillä voidaan myös monitoroida ja analysoida käyttäjien ja ohjelmistojen poikkeavaa käyttäytymistä (Rochford & Kavanagh & Bussa, 2016).

Joulukuussa 2017 julkaistun tutkimusraportin mukaan organisaatioilla on vaikeuksia havaita tietomurtoja. Jopa 80 prosenttia tietomurroista jää tietomurron kohteeksi joutuneilta organisaatioilta havaitsematta aikaisessa vaiheessa. (Kavanagh & Bussa 2017.) SIEM-järjestelmän avulla organisaatiolla on parempi mahdollisuus havaita mahdolliset poikkeamat ja tietomurrot aikaisemmin, jolloin niihin voidaan reagoida nopeammin ja pienentää niistä aiheutuvia haittoja ja kustannuksia. (Ponemon Institute 2017, 3).

3.6 Identiteetinhallinta organisaatiossa

Organisaatioissa on nykyään useita tietojärjestelmiä, joihin tietyllä käyttäjällä on identiteetti ja erilaisia käyttövaltuuksia. Identiteetinhallinnan tyypillisenä haasteena onkin se, miten hallita identiteettejä useiden tietojärjestelmien kokonaisuudessa. (Linden 2015, 41.) Samalla kun tiedon määrä kasvaa, kasvaa samojen tietojen käsittely eri järjestelmissä sekä tarve yhdistää eri tietojärjestelmissä olevia tietoja. Jos samojen henkilöiden samoja tietoja ylläpidetään ilman yhtenäistä suuntaa, johtaa se tiedon epäyhtenäisyyteen sekä aiheuttaa päällekkäistä ja ylimääräistä työtä. (Kuntaliitto 2013b, 3.)

Master data management (MDM) tarkoittaa prosessia, jonka tavoitteena on poistaa päällekkäistä ja turhaa, vähentämällä samojen tietojen moninkertaista käsittelyä (Kuntaliitto 2013b, 13). Ydintiedon hallinta on keskeinen osa identiteetinhallinnan arkkitehtuuria ja sen mukaan identiteettiin liittyville attribuuteille määritetään autoratiivinen lähde. Autoratiiviseksi lähteeksi kutsutaan tietojärjestelmää, josta kyseessä olevan attribuutin arvoa tämän jälkeen ylläpidetään ja muutetaan. Tiedon muuttamisen jälkeen, muuttuneet tiedot siirtyvät toisiin tietojärjestelmiin. (Linden 2015, 44.)

Usein esiintyy tarve tehdä jostakin autoratiivisesta lähteestä perusrekisteri eli keskitetty piste, jonka kautta uusi identiteetti perustetaan organisaatioon, ja josta se siirretään muihin tietojärjestelmiin. Ihanteellisessa tilanteessa kaikki organisaation tietojärjestelmät kuuluvat keskitettyyn identiteetinhallintaan, mutta yleensä siihen päästään harvoin. Toisaalta siihen ei välttämättä edes kannata pyrkiä, sillä integraatioiden rakentaminen ja ylläpitäminen maksavat. On tarkkaan harkittava, mitkä järjestelmät perusrekistereiden ja autoratiivisten lähteiden lisäksi kytketään identiteetinhallintajärjestelmään. (Linden 2015, 44–46.)

Identiteetinhallintajärjestelmän (IdM) ydin on metahakemisto, joka synkronoi organisaation eri käyttäjätietokannat keskenään. Parhaimmillaan metahakemiston avulla saadaan hoidettua koko identiteetin elinkaari. Kun metahakemisto havaitsee uuden identiteetin perusrekisterissä, se perustaa eli provisioi identiteetin muihin käyttäjätietokantoihin. Tämän lisäksi metahakemisto huolehtii muuttuvien tietojen, kuten työtehtävän tai roolin muutoksen päivittämisen kohdejärjestelmiin. Kun identiteetti suljetaan esimerkiksi eläköitymisen johdosta perusrekisterissä, huolehtii metahakemisto identiteetin sulkemisesta eli deprovisioinnista kohdejärjestelmissä. (Stackpole & Hanrion 2007, 161.) Metahakemisto huolehtii myös tarvittaessa tiedon muunnoksista lähde- ja kohdejärjestelmien välillä. Identiteetinhallintajärjestelmissä on yleensä useita liitäntöjä, joiden avulla identiteetit voidaan provisioida ja deprovisioida eri järjestelmiin. (Linden 2015, 50.)

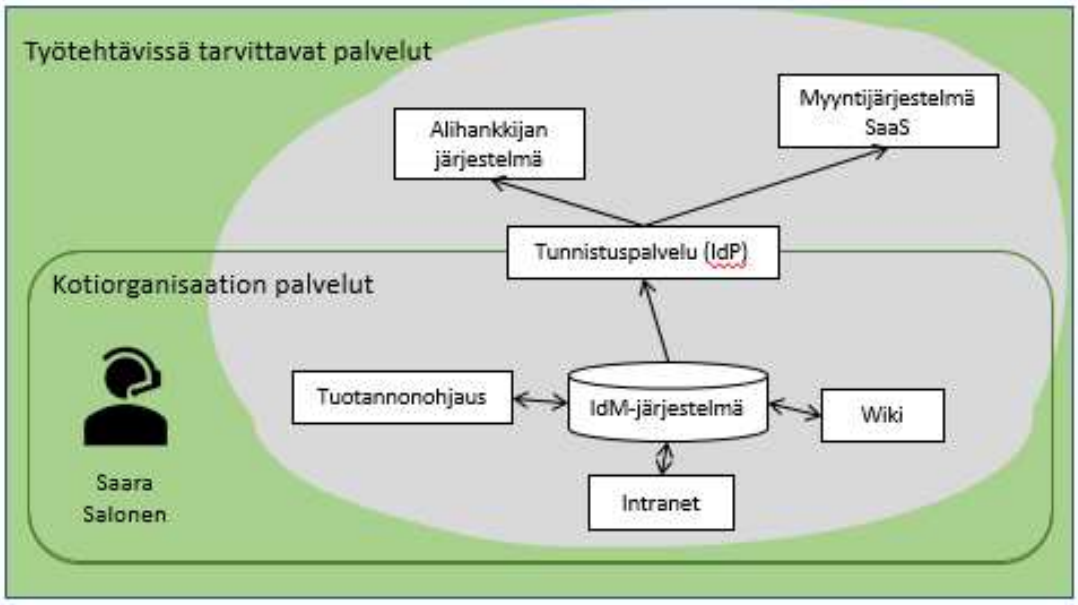
IDaaS-palvelut ovat käytännöllinen ratkaisu identiteettien provisiointiin (Wagner ym. 2015). Identiteettien provisioinnilla eri järjestelmiin voidaan myös vähentää hukattua työaikaa. Käyttäjät voivat alkaa käyttämään kaikkia tarvitsemiaan järjestelmiä heti, sillä heidän ei tarvitse odottaa tunnuksen luomista jokaiseen järjestelmään erikseen. (F5 2016.)

3.7 Federoitu identiteetinhallinta

Edellä tutustuttiin tilanteeseen, missä sekä identiteettiä että tietojärjestelmiä hallinnoitiin yhden ja saman organisaation toimesta. Nykypäivän verkostoituneen maailman tarpeet luovat kuitenkin koko ajan enemmän tilanteita, joissa identiteetin hallinnointi tapahtuu eri organisaatiossa. Esimerkiksi kun työntekijä joutuu kirjautumaan ulkoisen palvelutoimittajan järjestelmiin. Luottamusverkostoiden tarkoituksena on kasvattaa käyttäjän mahdollisuutta hyödyntää yhdellä identiteetillä useita eri palveluita. (Pfleeger ym. 2015e.)

Tässä alaluvussa kotiorganisaatioksi kutsutaan organisaatiota, jonka kanssa käyttäjällä on sidos, kuten oppilaitos tai työnantaja. Sidoksen myötä käyttäjällä voi olla käyttövaltuus muiden organisaatioiden ylläpitämiin järjestelmiin. Ulkopuolisten tietojärjestelmien identiteetin- ja pääsynhallinnan liittämistä organisaation sisäiseen identiteetinhallintajärjestelmään nimitetään federoiduksi identiteetinhallinnaksi (federated identity management). Sen tarkoitus ei ole korvata tai vähentää sisäisen identiteetinhallinnan merkitystä, päinvastoin se mahdollistaa myös organisaation ulkopuoliset palvelut sen piiriin. (Linden 2015, 53.)

Federoitussa identiteetinhallinnassa peruskomponentteja ovat tunnistuspalvelu (Identity Provider, IdP) ja tunnistukseen nojaava palvelu (Service Provider, SP tai Relying Party, RP). Tunnistuspalvelu on palvelin, jonka käytettävissä on ajantasaiset tiedot käyttäjien identiteeteistä ja joka suorittaa käyttäjien tunnistamisen kirjautumishetkellä. Käyttäjän kotiorganisaatioksi kutsutaan sitä organisaatioita, joka omistaa tunnistuspalvelun. Tunnistukseen nojaavaksi palveluksi kutsutaan sitä varsinaista sovellusta, joka tarvitsee käyttäjien tunnistusta ja joka nojaa pääsynvalvonnassa tunnistuspalvelun suorittamien käyttäjien tunnistuksiin ja sieltä saataviin käyttäjien attribuutteihin. (Pfleeger ym. 2015f.) Lähtökohtaisesti kirjautumishetkellä tunnistuspalvelusta saadaan käyttäjän ajantasaiset perustiedot (Linden 2015, 54). Federoitu identiteetinhallinta on esitetty kuviossa 4, jossa harmaa alue kuvastaa identiteetin kattavuutta.



Kuvio 4. Federoitu identiteetinhallinta (mukaillen Linden 2015, 53).

Federoidun identiteetinhallinnan hyödyt ovat pitkälti samoja kuin alaluvussa 3.1 esitellyt identiteetin- ja pääsynhallinnan kehittämisen hyödyt. Suurimpia haasteita federoidussa identiteetinhallinnassa on osapuolien välinen luottamus (Baldwin & Casassa Mont & Beres & Shiu 2010, 520). Identiteettien täytyy luottaa tunnistuspalveluun. Tunnistuspalvelun taas täytyy luottaa siihen, ettei tunnistukseen nojaavassa palvelussa loukata käyttäjän yksityisyyttä käyttäjästä välitettyjä attribuutteja käsiteltäessä. Tunnistukseen nojaavan palvelun täytyy luottaa siihen, että käyttäjä on tunnistettu tunnistuspalvelussa riittävän luotettavasti, ja että tunnistuspalvelun välittämät attribuutit ovat oikein ja ajan tasalla. (Baldwin ym. 2010, 528.)

Osapuolten täytyy hallita riskiä siitä, ettei vastapuoli ole sille annetun luottamuksen arvoinen (Baldwin ym. 2010, 521). Keskeisiä tapoja hallita luottamusriskiä ovatkin osapuolten kesken solmimat sopimukset federoituun identiteetinhallintaan liittyvistä velvollisuuksista ja oikeuksista. Luottamussuhteet voidaan rakentaa kahdenvälisiksi, keskitetyiksi luottamusverkostoiksi ja monenkeskisiksi luottamusverkostoiksi. (Linden 2015, 56–57.)

Suomessa yksityishenkilöiden vahva sähköinen tunnistaminen nojaa erityisesti pankkien Tupas-palveluun. Sen avulla sähköisiä asiointipalveluita tarjoavat organisaatiot voivat tunnistaa asiakkaansa luotettavasti. (Finanssialan Keskusliitto 2013, 4.) Muita vahvoja sähköisen tunnistamisen välineitä ovat mobiilivarmenteet ja Väestörekisterikeskuksen kansalais- ja organisaatiovarmenteet (Viestintävirasto 2016, 26). Vahvaa sähköistä tunnistamista sekä tunnistuspalveluiden tarjoamista säätelee laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 1 §).

Haka-verkosto on korkeakoulujen ja tutkimuslaitosten opiskelijoille, opettajille ja tutkijoille tuttu käyttäjätunnistusjärjestelmä. Sillä on noin 326 000 käyttäjää ja se perustuu luottamusverkostoon. Verkoston jäsenet voivat käyttää kotiorganisaationsa käyttäjätunnuksia kirjautuessaan moniin eri Haka-tunnistukseen nojaaviin palveluihin. Palveluihin lukeutuvat muun muassa oppimisalustat, korkeakoulukirjastojen sähköiset palvelut ja tutkimusresurssit. (Laalo 2017.)

Virtu on valtion virastojen luottamusverkosto. Sen kautta virkamiehet voivat käyttää kertakirjautumista Virtu-verkostoon liitettyihin viraston omiin ja valtion yhteisiin selainpohjaisiin järjestelmiin. (Valtori 2016.)

3.8 Henkilötietolaki ja EU:n tietosuoja-asetus

Koska tietojärjestelmien käyttäjätietokannassa olevat identiteetit voidaan yleensä yhdistää luonnollisia henkilöitä koskeviksi merkinnöiksi, täyttyy henkilötiedon määritelmä. Käyttäjätietokanta tulkitaan näin ollen henkilörekisteriksi. Käyttäjätietokannan omistajaa kutsutaan rekisterinpitäjäksi ja käyttäjää rekisteröidyksi. Henkilötietojen käsittelyksi kutsutaan kaikkia käyttäjätietoihin kohdistuvia toimia. (Linden 2015, 63.)

Rekisterinpitäjän tulee toteuttaa tarpeelliset organisatoriset ja tekniset toimenpiteet, joilla henkilötiedot suojataan asiattomalta pääsyltä. Rekisterinpitäjän on suojattava henkilötiedot sekä vahingossa että laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta sekä muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa tulee huomioida käytettävissä olevat tekniset mahdollisuudet sekä mahdollisista toimenpiteistä aiheutuvat kustannukset. Toteutettaviin toimenpiteisiin vaikuttavat käsiteltävänä olevien tietojen laatu, niiden määrä ja käsittelyn merkitys yksityisyyden suojaan. (Henkilötietolaki 1999, 32 §.)

Rekisteröidyn yksityisyyden suojan kannalta erityisen arkaluonteisia tietoja ovat muun muassa merkinnät rekisteröidyn rodusta tai etnisestä alkuperästä, yhteiskunnallisesta tai poliittisesta vakaumuksesta, rangaistuksesta, rekisteröidyn terveydentilasta, hänen sairaudesta tai häneen kohdistetuista hoitotoimenpiteitä, seksuaalisesta suuntautumisesta tai sosiaalihuollon tarpeista. (Henkilötietolaki 1999, 11 §.) Arkaluontoisia henkilötietoja saa käsitellä vain laissa olevien poikkeuksin (Henkilötietolaki 1999, 12 §).

Euroopan unionin tietosuojalainsäädäntö uudistui yleisen tietosuoja-asetuksen astuessa voimaan 24. toukokuuta 2016. Tietosuoja-asetusta sovelletaan kahden vuoden siirtymäajan jälkeen 25. toukokuuta 2018 alkaen. Tämän jälkeen henkilötietoja tulee käsitellä tietosuoja-asetuksen mukaisesti. (Oikeusministeriö 2017, 9.)

Henkilötietojen käsittelyn laajuus on muuttunut paljon viime vuosina. Tietosuoja-asetuksen tarkoitus on saattaa tietosuojaa koskeva sääntely ajan tasalle ja harmonisoida jäsenvaltioiden tietosuojasäännökset yhdenmukaisiksi. Asetuksella pyritään lisäämään henkilötietojen käsittelyn läpinäkyvyyttä ja avoimuutta sekä vahvistamaan rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. (Oikeusministeriö 2017, 9; Valtiovarainministeriö 2016b, 6.)

Tietosuoja-asetuksen velvoitteiden noudattamista tuetaan tehokkaalla täytäntöönpanolla. Asetuksen vastaisesta henkilötietojen käsittelystä on säädetty henkilötietolakia tiukemmat seuraamukset. Valvontaviranomaiset voivat määrätä henkilötietojen käsittelyyn liittyviä sakkoja ja korjaavia toimenpiteitä. (Oikeusministeriö 2017, 9.) Sakon suuruus voi olla jopa 20 miljoonaa euroa tai 4 prosenttia vuosittaisesta maailmanlaajuisesta kokonaisliikevaihdosta (Valtiovarainministeriö 2016b, 7).

Tietosuoja-asetus koskee kaikkia sen soveltamisalaan kuuluvia rekisterinpitäjiä ja henkilötietojen käsittelijöitä. Sitä sovelletaan yksityisellä ja julkisella sektorilla, tietyissä tilanteissa myös EU:n ulkopuolella sijaitseviin organisaatioihin. (Oikeusministeriö 2017, 9.)

Tietosuoja-asetusta sovelletaan automaattisen henkilötietojen käsittelyn lisäksi henkilötietojenkäsittelyyn, kun henkilötiedot muodostavat rekisterin osan. Asetus ohjaa rekisterinpitäjää käsittelemään henkilötietoja niin, että rekisteröidyn oikeuksia ja vapauksia kunnioitetaan. Rekisterinpitäjän tulee lisäksi huolehtia, että kaikissa henkilötietojen käsittelyvaiheissa noudatetaan tietosuojaperiaatteita. Rekisterinpitäjän osoitusvelvollisuuden johdosta rekisterinpitäjän tulee pystyä osoittamaan, että asetusta noudatetaan henkilötietojen käsitellyssä. Lisäksi rekisterinpitäjän on pystyttävä osoittamaan toteuttavansa tietosuojaperiaatteita käytännössä. (Valtiovarainministeriö 2016b, 18.)

Jos tietojen käsittelyyn liittyviä tehtäviä ulkoistetaan henkilötietojen käsittelijälle, tulee henkilötietojen käsittelijän antaa riittävät takeet siitä, että henkilötietoja käsitellessään henkilötietojen käsittelijä täyttää asetuksen vaatimukset (Oikeusministeriö 2017, 22). Rekisterinpitäjän ja henkilötietojen käsittelijän välillä on suotavaa olla kirjallinen sopimus, jossa määritellään mitä henkilötietoja käsitellään, miksi ja minkä ajan (Valtiovarainministeriö 2016b, 28).

Rekisterinpitäjän velvollisuus on ottaa huomioon rekisteröidyn oikeudet henkilötietojen käsittelyssä. Tietosuoja-asetuksessa korostetaankin henkilötietojen käsittelyn osalta avoimuutta. Asetuksessa annetaan lisäksi määräyksiä rekisteröidyn oikeuksien ja rekisterinpitäjän informointivelvollisuuden toteuttamisesta. Rekisterinpitäjän tulee toimittaa rekisteröidylle henkilötietojen käsittelyyn liittyvät tiedot. Tiedot tulee toimittaa helposti ymmärrettävässä muodossa. Lisäksi asetus takaa rekisteröidylle oikeuden saada jäljennöksen häntä koskevista henkilötiedoista ja takaa tietyin poikkeuksin oikeuden tietojen poistamiseen. Tätä kutsutaan myös oikeudeksi tulla unohdetuksi. (Oikeusministeriö 2017, 23–25; Valtiovarainministeriö 2016b, 14–18.)

Tietosuoja-asetuksessa säädetään uutena asiana rekisterinpitäjän velvollisuudesta ilmoittaa tietoturvaloukkauksista sekä tietosuojaviranomaiselle että rekisteröidyille. Tietoturvaloukkaus tarkoittaa tapahtumaa, jonka seuraus on henkilötietojen tuhoaminen, niiden muuttaminen, häviäminen, luvaton luovuttaminen tai pääsy kyseisiin henkilötietoihin. (Oikeusministeriö 2017, 32; Valtiovarainministeriö 2016b, 17.) Täyttääkseen ilmoitusvelvollisuuden tulee rekisterinpitäjällä olla kyvykkyys havaita poikkeamat ympäristössään,

selvittää havaittujen poikkeamien syyt sekä mahdolliset seuraukset ja vaikutukset yksityisyydensuojaan (Valtiovarainministeriö 2016b, 26–27).

Suomessa tietoturvaloukkauksia, kuten henkilötietoihin liittyviä tietomurtoja, koskeva rekisterinpitäjän ilmoitusvelvollisuus ei ole uusi asia. Tietoyhteiskuntakaaressa säädetään teleyrityksen velvollisuudesta ilmoittaa Viestintävirastolle, jos yrityksen palvelua uhkaa tai siihen kohdistuu merkittävä tietoturvaloukkaus (Tietoyhteiskuntakaari 2014, 275 §). Saman lain mukaan teleyrityksellä on tietyissä tilanteissa velvollisuus ilmoittaa merkittävästä tietoturvaloukkauksesta myös käyttäjille (Tietoyhteiskuntakaari 2014, 274 §).

4 Toteutus

Opinnäytetyön tarkoituksena on selvittää asiakastarpeet ja alustavasti valittujen ohjelmistotuotteiden soveltuvuus vastaamaan asiakastarpeita. Selvitys tehdään osana toimeksiantajan identiteetin- ja pääsynhallintapalvelun tuotteistamisprojektia. Toimeksiantaja, Citrus Solutions Oy, on panostanut viime vuosina vahvasti tietosuoja- ja tietoturvapalveluihin. Toimeksiantaja on panostanut osa-alueisiin sekä orgaanisen kasvun (tietoturva-asiantuntijoiden palkkaus) että yritysoston (Digital Identity Solutions Europe Oy) kautta.

Digital Identity Solutions Europe Oy:n uusi nimi on Citrus Secure Identity Oy. Yrityksen palvelutarjoomaan sisältyy tuote (CSI Datamaster), joka mahdollistaa master datan eli ydintiedon hallinnan. Lisäksi siihen saadaan erillisinä lisäpalveluina liitettyä pääsynhallinta, lokienhallinta sekä kulunvalvonta.

Citrus Solutions Oy:n palveluihin kuuluu myGDPR-palvelu, joka auttaa asiakasta alkuun EU:n tietosuojavaatimusten täyttämisessä. SoteGDPR on laajennus edelliseen palveluun ja se ottaa EU:n tietosuoja-asetuksen vaatimusten lisäksi huomioon kansallisen sosiaali- ja terveydenhuollon lainsäädännön. Palvelun varsinaisina tutkittavina kohteina ovat sosiaalihuollon asukas/asiakastiedot ja terveydenhuollon potilastiedot.

Toimeksiantajan kanssa käytyjen keskustelujen ja sähköpostiviestien pohjalta voidaan todeta, että toimeksiantaja on havainnut asiakkaillaan olevan tarvetta identiteetin- ja pääsynhallintapalvelulle. Toimeksiantaja on havainnut, että asiakkailla on tarve vähentää eri

palveluiden käyttöön tarvittavien tunnusten ja salasanojen määrää. Asiakkailla on havaittu myös tarve parempiin käytäntöihin tunnusten perustamisen ja lopettamisen osalta. Lisäksi asiakkailla on tarve tehostaa toimintaa vähentämällä salasanojen nollauspyyntöjä lähitukeen sekä vähentämällä henkilötietojen moninkertaista käsittelyä eri järjestelmissä.

Lisäksi asiakkailla on havaittu tarve kertakirjautumisjärjestelmälle, jota on mahdollista käyttää myös mobiililaitteilla. Osaan palveluista on havaittu tarve vahvalle tunnistautumiselle. Jotta uusien palveluiden käyttöönotto käy nopeasti, tulisi mahdollisessa ratkaisussa olla valmiina useita liitäntöjä eri järjestelmiin.

Toukokuussa sovellettavaksi tulevan EU:n tietosuoja-asetuksen osalta asiakkailla on havaittu tarve valmistautua asetuksen asettamiin vaatimuksiin ja heillä on tarve parempiin käytäntöihin ylläpitotunnusten käytön osalta. Lisäksi asiakkailla on tarve käyttäjätunnusten ja käyttöoikeuksien paremmalle raportoinnille sekä paremmalle jäljitettävyydelle oikeuksien käytön ja pääsyn osalta.

On myös havaittu, että asiakkailla on tarve ratkaisulle, jonka avulla he voisivat käyttää vaihtoehtoisia palveluita ja päästää ulkopuolisia luotettuja tahoja omiin palveluihinsa. Ratkaisun tulisi skaalautua asiakkaiden nykyisiin ja tuleviin tarpeisiin. Lisäksi hallinnan tulisi olla keskitetty.

Asiakastarpeet kartoitettiin kvalitatiivisilla haastatteluilla, sillä ne ovat suositeltavampia kuin lomakekyselyt. Haastattelut sallivat lomakekyselyitä paremmin haastateltavien omien ajatusten esiintulon. Lisäksi lomakekyselyiden heikkoutena on taipumus ohjata vastaajan ajatuksia ja rajoittaa käsiteltäviä teemoja kysymysten ja vastausvaihtoehtojen osalta. (Kinnunen 2004, 43.) Haastatteluilla pyrittiin lisäksi saamaan esille asiakkaiden mahdolliset uudet ja piilevät tarpeet.

Haastateltavat asiakasorganisaatiot (Lapin sairaanhoitopiiri, Turun Kaupunki ja Citrus Solutions Oy) valittiin siten, että ne olivat käyttäjämääriltään erikokoiset ja siten tarpeiltaan erilaiset. Toimeksiantaja on mukana haastateltavien joukossa, sillä heillä on havaittu asiakasorganisaatioiden kanssa samankaltaisia tarpeita.

Asiakasorganisaatiot nimesivät haastateltavat henkilöt. Tällä pyrittiin varmistamaan, että haastateltaviksi valikoituvat ne henkilöt, joilta saadaan eniten tietoa asiakastarpeista.

Joissakin tapauksissa tällaisella niin sanotulla lumipallomenetelmällä tehdyillä valinnoilla on vaarana johtaa vinoutuneisiin tutkimustuloksiin, jos nimeävä henkilö ei halua nimetä omia mielipiteitään vastaan olevia vastaajia (Kananen 2014, 97–98). Tällaisesta aineiston vinoutumisesta ei ole havaintoja, mutta sitä ei voida kokonaan poissulkea.

Jotta tiedon reliabiliteettia ja validiteettia voitiin parantaa, noudatettiin haastatteluissa toimintamallia, jolla varmistettiin, että kaikille haastateltaville esitettiin samankaltaiset kysymykset. Haastatteluiden kysymykset tuotettiin yhteistyössä toimeksiantajan kanssa. Opinnäytetyön tekijä teki ensimmäisen kysymyslistan, jota toimeksiantaja kommentoi. Tämän jälkeen kysymyksiä muokattiin kommenttien perusteella ja päivitetyt kysymykset esitettiin toimeksiantajalle. Tätä jatkettiin, kunnes molemmat osapuolet olivat tyytyväisiä kysymyslistaan.

Tärkeintä haastatteluissa on kerätä mahdollisimman paljon tietoa tutkittavasta asiasta. Haastattelun onnistumisen kannalta on suotavaa antaa haastateltavien tutustua aiheisiin ja kysymyksiin ennen haastattelua. (Tuomi & Sarajärvi 2002, 75.) Tämän vuoksi haastattelurunko toimitettiin haastateltaville etukäteen saatteen kanssa. Haastattelun saate on esitetty liitteessä 1 ja haastattelurunko liitteessä 2.

Haastattelut kestivät 50 ja 85 minuuttia ja ne suoritettiin kolmena yksilöhaastatteluna ja yhtenä viiden hengen ryhmähaastatteluna. Ryhmähaastattelun keskeinen etu yksilöhaastatteluun nähden on se, että ryhmähaastattelulla saadaan nopeasti ja samanaikaisesti tietoa usealta henkilöltä. Lisäksi ryhmän jäsenet auttavat toisiaan muistamaan sellaisia asioita, joita ei välttämättä muistaisi yksilöhaastattelussa. (Ojansalo & Moilanen & Ritalahti 2015, 41–42.) Ryhmähaastattelussa ongelmaksi saattaa syntyä se, että kaikkien mielipide ei tule esille, jos ryhmässä on yksi tai kaksi dominoivaa henkilöä (Hirsjärvi & Hurme 2008, 63). Ryhmähaastattelun aikana kyseistä ongelmaa ei ollut juuri havaittavissa.

Haastattelujen aikana kysymyksiä ei esitetty missään tietyssä järjestyksessä vaan ne esitettiin haastattelun aikana sellaisena hetkenä kuin oli luontevaa. Lisäksi haastatteluun soveltumattomat kysymykset jätettiin esittämättä. (Ojansalo ym. 2015, 108.) Puolistrukturoiduille haastatteluille onkin ominaista, että haastattelun kaikkia näkökulmia ei ole lyöty lukkoon (Hirsjärvi & Hurme 2008, 47).

Haastateltaville annettiin mahdollisuus vastata kysymyksiin vapaasti ja jakaa kaikki heillä oleva tieto. Haastateltavia pyrittiin olemaan keskeyttämättä ja heiltä pyrittiin tiedustelemaan lisää, jos jokin asia jäi epäselväksi. (Kananen 2015, 83–85.) Tavoitteena oli lisätä haastattelujen kautta saadun tiedon laatua.

Haastattelut suoritettiin kasvokkain tai käyttämällä kuvallista videoyhteyttä. Haastattelut tallennettiin haastateltavien luvalla ja niistä tehtiin yhteenveto litteroinnin perusteella. Litterointi tehtiin mahdollisimman nopeasti haastattelun jälkeen, jotta käsitellyt teemat olisivat mahdollisimman hyvin muistissa. Koska haastatteluilla kerättiin sellaista aineistoa, jossa vain vastausten sisällöillä oli merkitystä, suoritettiin litterointi käyttämällä yleiskieltä (Ojasalo ym. 2015, 107). Yhteenvedot lähetettiin haastateltaville, jotka tarkistivat sisällön ja tekivät omat huomionsa ja korjausehdotuksensa. Jos tiedon analysoinnin aikana nousi esille joitakin lisäkysymyksiä, ne esitettiin sähköpostitse haastateltaville.

Haastatteluista kertynyt aineisto luettiin useaan kertaan läpi paremman kokonaiskuvan saamiseksi. Aineiston analysoinnissa käytettiin induktiivista aineistolähtöistä sisällönanalyysiä. Tämän aikana aineisto pelkistettiin ja yhteen kuuluvat vastaukset yhdistettiin, ensin teemoittain ja sen jälkeen kysymyksittäin. Sisällönanalyysin aikana aineistosta etsittiin asiakastarpeita ja niitä verrattiin alkuperäisiin havaintoihin.

Vertaamalla aiemmin tehtyjä havaintoja asiakastarpeista suhteessa Micro Focuksen ja toimeksiantajan ohjelmistoista löytyviin ominaisuuksiin, voidaan havaita, että useisiin asiakastarpeisiin pystytään vastaamaan. Tukeakseen tekemiään päätelmiä Micro Focuksen ohjelmistojen soveltuvuudesta, opinnäytetyön tekijä tutustui Micro Focuksen internetsivuihin, ohjelmistojen ohjeistuksiin sekä eri tutkimuslaitosten tekemiin raportteihin, jotka liittyivät identiteetin- ja pääsynhallinnan kokonaisarkkitehtuuriin.

Jotta päätelmät Micro Focuksen ohjelmistojen soveltuvuudesta olisivat mahdollisimman paikkansapitävät, asiakastarpeet ja tehdyt päätelmät käytiin läpi Micro Focus Suomen edustajan Pekka Lindqvistin (2018) kanssa. Toimeksiantajan CSI Datamaster-ohjelmistoa käsittelevät päätelmät käytiin läpi Principal Consultant Pasi Taimisen (2018) kanssa. Näiden keskustelujen pohjalta tehtiin joitakin muutoksia päätelmiin ohjelmistojen soveltuvuuden osalta. Tehdyt havainnot asiakastarpeista ja ohjelmistojen soveltuvuudesta vastaamaan näihin tarpeisiin on koostettu toimeksiantajalle tehtyyn selvitykseen. Selvitys on esitetty opinnäytetyön liitteessä 3.

5 Tuotos

Opinnäytetyön tuotoksena valmistui selvitys asiakastarpeista ja toimeksiantajan alustavasti valitsemien ohjelmistojen soveltuvuudesta vastaamaan asiakastarpeisiin. Toimeksiantaja voi käyttää selvitystä käynnissä olevassa identiteetin- ja pääsynhallinnan tuotteistamisprojektissaan. Selvityksessä on käytetty jonkin verran kuvia teemojen havainnollistamiseksi ja jotta se olisi miellyttävämpi lukea. Selvityksessä käytetyt kuvat ovat ohjelmistotoimittaja Micro Focuksen internetsivuilta.

Selvitys alkaa johdannolla. Sen jälkeen luvussa 2 esitetään, kuinka aineisto on kerätty ja millaisilla menetelmillä sitä on käsitelty. Koska selvitys on tehty osana toimeksiantajan identiteetin- ja pääsynhallinnan tuotteistamisprojektia, ei selvityksessä käydä läpi tuotteistamista eikä identiteetin- ja pääsynhallinnan perusteita. En kokenut niiden sisällyttämistä selvitykseen tarkoituksenmukaiseksi. Toimeksiannon mukaisesti selvityksessä on tarkoitus keskittyä asiakastarpeiden selvittämiseen ja tuotteiden soveltuvuuden varmistamiseen.

Luvussa 3 käydään läpi havaitut asiakastarpeet haastattelurungon teemojen mukaisesti. Jokaiselle teemalle on oma otsikkonsa. Luku 4 käsittelee ohjelmistojen soveltuvuutta vastata luvussa 3 esitettyihin havaintoihin asiakastarpeista. Jokaisen teeman osalta tulokset käydään läpi oman otsikon alla. Luvussa 4 olen kuitenkin tehnyt muutamia muutoksia otsikoiden ja teemojen suhteen. Käyttäjätunnusten, roolien ja oikeuksien perustaminen ja poistaminen käsitellään yhden otsikon alla.

Luvussa 5 esitellään huomiot koskien hinnoittelumallia, joilla haastateltavat voisivat hankkia identiteetin- ja pääsynhallintapalvelun pilvipalveluna. Selvityksen lopuksi luvussa 6 käydään läpi johtopäätökset.

5.1 Tavoitteiden saavuttaminen ja analysointi

Opinnäytetyön tuotoksena valmistunut selvitys on yksi osa toimeksiantajan asiakaslähtöistä identiteetin- ja pääsynhallinnan tuotteistamisprojektia. Oletan, että selvitys ei paljastanut toimeksiantajalle mitään täysin uutta ja odottamatonta asiakastarvetta. Selvityksen avulla saatiin kuitenkin pitkälti vahvistettua oletetut asiakastarpeet. Havaittujen asiakastarpeiden vertaaminen alustavasti valittujen ohjelmistojen ominaisuuksiin paljasti,

että asiakastarpeisiin pystytään vastaamaan hyvin. Mielestäni tämä vahvistaa sen, että toimeksiantaja voi käyttää selvitystä apunaan tuotteistamisprojektin päätösten osalta. Samoin toimeksiantaja voi käyttää selvityksen avulla saatuja tietoja suunnitellessaan palvelutuotteen sisältöä ja vakioinnin astetta.

Jotta selvityksestä olisi saatu kattavampi, olisi asiakkaiden organisaatioihin ja eri järjestelmiin pitänyt tutustua hyvin tarkasti. Tämä olisi vaatinut niin suurta työmäärää ja erillisiä salassapitosopimuksia asiakasorganisaatioiden kanssa, ettei se ollut tämän opinnäytetyön puitteissa mahdollista. Lisäksi selvityksen kattavuutta rajoittaa se, että tietoturvasyistä johtuen asiakasorganisaatiot eivät voineet kertoa kaikista asioista yksityiskohtaisesti. Riskinä on erilaisille tietoturvauhille altistuminen, jos tietoturva-asioita käsitellään liian tarkasti. Näistä rajoitteista huolimatta sain mielestäni haastatteluiden avulla selvitettyä asiakkaiden pääasialliset tarpeet identiteetin- ja pääsynhallinnan kokonaisuuden osalta.

Selvityksen rajoitteista huolimatta oletan toimeksiantajan saaneen selvityksen avulla vahvistuksen sille, että he ovat oikealla tiellä tuotteistamisprojektinsa kanssa. Lisäksi oletan, että asiakasorganisaatioiden edustajat arvostavat toimeksiantajan halua kuunnella asiakkaidensa ääntä tuotteistamisprojektinsa aikana. Näin asiakkaiden tarpeisiin voidaan vasta paremmin.

6 Johtopäätökset

Opinnäytetyön tarkoituksena oli osana tuotteistamisprojektia selvittää asiakastarpeet ja arvioida alustavasti valittujen ohjelmistotuotteiden soveltuvuus vastaamaan näihin asiakastarpeisiin. Koska tämä on vain pieni osa koko tuotteistamisprojektia, ei opinnäytetyön tuloksia voida kokonaisuudessaan yhdistää tuotteistamisen viitekehykseen. Koko tuotteistamisprosessin viitekehyksen jättäminen esittämättä ei myöskään olisi ollut mielekästä. Tämä on yksi syy siihen, miksi koko asiakaslähtöinen tuotteistamisprosessi on esitetty viitekehyksessä. Toinen syy tuotteistamisprosessin esittelylle on se, että lukijalle muodostuisi tarkempi käsitys siitä mistä kaikesta tuotteistaminen koostuu.

Opinnäytetyön teoriaosuudessa esitetty asiakaslähtöinen tuotteistamismalli antaa mielestäni yrityksille paremman mahdollisuuden onnistua tuotteistamisprojekteissaan.

Kaikki lähtee liikkeelle siitä, että uusien palveluiden tulee olla yrityksen liiketoimintastrategian mukaisia (Jaakkola ym. 2009, 8). Toimeksiantajan tekemät viime aikaiset panostukset tietosuoja- ja tietoturvapalveluihin kertovat siitä, että tuotteistusprojektin kohteena oleva identiteetin- ja pääsynhallinta on tärkeä osa tämän hetkistä liiketoimintastrategiaa.

Maksava asiakas viimekädessä päättää sen, onko jokin palvelutuote sellainen, josta hän on valmis maksamaan (Edvardsson & Olsson 1996, 141–142). Yritysten tuleekin lähteä liikkeelle siitä, että uudella palvelulla kyetään vastaamaan asiakkaan piileviin tai tiedossa oleviin tarpeisiin. Toimeksiantajalla oli alustavat oletukset asiakkaiden tarpeista, joiden pohjalta he olivat suunnitelleet uutta palvelua. Jotta palvelun sisältö saadaan parhaalla mahdollisella tavalla vastaamaan asiakastarpeita, tulee ne saada kartoitetuksi.

Asiakaslähtöisessä tuotteistamisessa asiakkaiden ottaminen mukaan tuotteistamiseen onkin keskiössä, jotta uusi palvelu vastaisi mahdollisimman hyvin asiakkaiden tarpeisiin. Alam ja Perry (2002, 533) ovatkin tutkimuksessaan todenneet, että asiakkaiden osallistaminen on tärkeää palvelun suunnittelussa. Selvitystä varten suoritetuilla haastatteluilla pyrittiin saamaan asiakasnäkökulma mukaan palvelun suunnitteluvaiheeseen. Toimeksiantajan on mahdollista käyttää selvitystä tehdessään tarkennuksia palvelun sisältöön. Lisäksi selvityksen tuloksia on mahdollista käyttää apuna palvelun vakioinnin ja räätälöinnin välisen suhteen suunnittelussa.

Identiteetin- ja pääsynhallinnan teoreettisessa viitekehyksessä aihetta käytiin läpi hyvin laajasti, sillä halusin perehtyä kokonaisuuteen mahdollisimman perusteellisesti. Laajaan kokonaisuuteen kuuluvat asiat nousivat esille haastattelujen aikana. Teoriaosuudessa kerrottiin, että identiteetinhallinnan suurena ongelmana on, ettei käyttäjän käyttövaltuuksia muisteta poistaa, kun perusteet käyttövaltuuksille lakkaavat olemasta. Osa haastateltavista tunnisti tämän ongelmaksi, kun toiset taas eivät. Tästä voidaan mielestäni päätellä, että osa organisaatioista on ottanut käyttöön paremmat prosessit käyttäjätunnusten auditointeihin. Mielestäni organisaatioiden tulisi ottaa säännölliset auditoinnit osaksi tietoturvakäytäntöjään. Toivon, että EU:n tuleva tietosuoja-asetus saa organisaatiot muuttamaan käytäntöjään.

Hyvin toimiva identiteetin- ja pääsynhallintajärjestelmä onkin tärkeä osa EU:n tietosuoja-asetuksen velvoitteisiin vastaamisessa. Sen avulla organisaatio mahdollistaa rajatun ja hallitun pääsyn henkilötietoihin, joiden käsittelyä säädetään tällä hetkellä henkilötieto-

lailla. Jatkossa kaikkien henkilötietojen käsittelyyn sovelletaan tietotuoja-asetusta. Voidaankin todeta, että identiteetin- ja pääsynhallinta tulisi nähdä olevan tietosuojan keskiössä.

Identiteetin- ja pääsynhallintajärjestelmän käyttöönotolla organisaation on myös mahdollista toimia tehokkaammin karsimalla ja automatisoimalla turhia työvaiheita (Linden 2015, 7). Selvityksen perusteella haastateltavat olivat samaa mieltä. Lisäksi samalla tiedon laatu ja tietoturva paranevat, kun inhimillisten virheiden mahdollisuus vähenee tietojen syöttämisessä ja poistamisessa. Nykyisessä modernissa maailmassa kaikki manuaalinen, turha ja virhealtis työ pyritään automatisoimaan. Kuten useampi haastateltava kertoi, niin automatisointia tulee tavoitella mahdollisimman paljon. Herääkin kysymys miksi tietojen siirtämistä järjestelmästä toiseen ei kannattaisi pyrkiä automatisoimaan?

Kuten haastatteluissa tuli esille, järjestelmätoimittajilta ja myyjiltä tiedusteltaessa mitä SIEM-järjestelmä tarkoittaa, tuntuu jokaiselta saavan vähän eri vastauksen. On harhaluulo, että pelkkä lokitietojen kerääminen ja yksinkertainen yhdistäminen tarkoittaa kyseessä olevan SIEM-järjestelmä. Usein organisaatiot aloittavat lokitietojen keräämisen verkkolaitteista, kuten palomuureista. Se on toki hyvä alku, mutta lokitietoja tulisi kerätä myös muista lähteistä. Lisäksi lokitietojen keskittäminen on vasta ensimmäinen askel. SIEM-järjestelmän tulee pystyä korreloimaan tietoa, analysoimaan tapahtumia sekä tehdä niiden perusteella päätelmiä lokitiedoista löytyvistä tiedonjyvistä. (Lipsman 2017.) Esimerkiksi toimeksiantajan SaaS-palveluna tarjoamalla SIEM-ratkaisulla näin pystyttäisiin tekemään.

Luottamusverkostojen kautta verkoston jäsenet voivat luotettavalla tavalla käyttää toistensa palveluita. Koska organisaatio itse vastaa omien käyttäjien tietojen ajantasaisuudesta ja oikeuksista, on heillä paras mahdollisuus huolehtia siitä kuka saa käyttää mitäkin palvelua. Jos organisaatio hankkii identiteetin- ja pääsynhallinnan ulkopuoliselta organisaatiolta palveluna (IdaaS), menettää se osan tästä hallinnasta, sillä organisaatiolla ei ole tarkkaa tietoa siitä, kuinka palveluntarjoajan prosessit toimivat ja kuinka palveluntarjoaja turvaa identiteetit (Bedell 2012). Nämä ovat riskejä, joiden hyvät ja huonot puolet organisaatioiden tulee punnita.

Toimeksiantajan tulee varmistaa turvallinen identiteettien käsittely. Kyseiseen haasteeseen pystytään vastaamaan selvityksessä esitetyllä kolmitasoisella välitysmallilla (Bro-

ker-malli). Käyttäjän pyrkiessä sisään johonkin kohdesovellukseen, tarkistaa välityspalvelin käyttäjän tunnuksen olemassaolon, voimassaolon, käyttäjän roolin sekä palvelun käyttöoikeuden takaisinkytkennällä käyttäjän kotiorganisaatiosta. Tunnistuspalvelun ja tunnistukseen nojaavan palvelun välillä välitetään vain kyseisen palvelun käyttöön tarvittavat tiedot käyttäjästä. Tämä mahdollistaa tietojen turvallisen käsittelyn.

Broker-malli mahdollistaa myös lokitietojen keräämisen ja raportoinnin. Näin käyttäjille voidaan toimittaa käyttöä koskevat tiedot. Tämän avulla käyttäjät saavat helposti selville palveluiden käyttöasteen ja voivat tarpeen tulleen todistaa kuka on käyttänyt mitäkin palvelua jonain tiettynä ajankohtana. Se auttaa siten osaltaan asiakasorganisaatioita selviytymään tietosuoja-asetuksen 72 tunnin ilmoitusvelvollisuudesta. Palveluntarjoajille voidaan tarjota käyttöä koskevaa raportointia laskutuksen tueksi (Mäntykangas 2018a).

Kuten jo selvityksen analysoinnissa mainittiin, haastateltavat eivät voineet tietoturvasyistä johtuen kertoa kaikista asioista kovin yksityiskohtaisesti. Riskinä olisi erilaisille tietoturvauhille altistuminen. Tämä avaakin mahdollisuuden jatkaa tuotteen kehittämistä asiakkaiden kanssa, kun palvelun ensimmäinen versio saadaan asiakkaille testausvaiheeseen. Kun isoimmat esille nousseista asiakastarpeista on ratkaistu, olisi mielenkiintoista osallistua uusien esille tulevien asiakastarpeiden selvittämiseen.

Kokonaisuutena opinnäytetyön tekeminen oli hyvin opettavainen matka. Oli mielenkiintoista perehtyä tuotteistamiseen sekä identiteetin- ja pääsynhallinnan eri osa-alueisiin. Vaikka matkan aikana opin molemmista aiheista paljon, niin vielä on paljon opittavaa. Toivottavasti pääsen tulevaisuudessa tekemään töitä molempien aiheiden parissa. Lopuksi haluan vielä kiittää toimeksiantajaa Citrus Solutions Oy:tä mahdollisuudesta osallistua projektiin ja erityisesti Ilpo Mäntykangasta, joka aina tarvittaessa auttoi, ohjasi ja opasti opinnäytetyön kanssa.

Lähteet

Alam, Ian & Perry, Chad 2002. A customer-oriented new service development process. Journal of Services Marketing. Vol. 16 Issue6, 515–534.

Apunen, Antti 2010. Tuotteistajan opas taloushallinnon asiantuntijalle. Suomen Taloushallintoliitto ry, Helsinki.

Baldwin, Adrian & Casassa Mont, Marco & Beres, Yolanta & Shiu, Simon 2010. Assurance for federated identity management. Journal of Computer Security 18, 2010. 519–550.

Bedell, Crystal 2012. Understanding IDaaS: The benefits and risks of Identity as a Service. TechTarget, Newton. Http://searchcloudsecurity.techtarget.com/feature/Understanding-IDaaS-The-benefits-and-risks-of-Identity-as-a-Service. Luettu 10.1.2018.

Bertino, Elisa & Takahashi, Kenji 2011. Identity Management. Concepts, Technologies, and Systems. Artech House, Norwood.

Coyne, Ed & Weil, Timothy R. 2013. ABAC and RBAC: Scalable, Flexible, and Auditable Access Management. IEEE IT Professional May/June 2013, 14–16.

Edvardsson, Bo & Olsson, Jan 1996. Key concepts for new service development. The Service Industries Journal; Apr 1996; 16, 2; ABI/INFORM Global. 140–164.

Edvardsson, Bo & Gustafsson, Anders & Kristensson, Per & Magnusson, Peter & Matthing, Jonas 2006. Involving customers in new service development. Imperial Vollege Press, London.

F5 2016. The Challenges and Benefits of Identity and Access Management. Whitepaper. Https://f5.com/resources/white-papers/the-challenges-and-benefits-of-identity-and-access-management-17862. Luettu 5.12.2017.

Finanssialan Keskusliitto 2013. Pankkien Tupas-tunnistuspalvelun tunnistusperiaatteet V2.0c 2.12.2013. Finanssialan Keskusliitto, Helsinki.

Flynn, Matt 2012. Identity and Access Management: Filling the Gap in Identity and Access Governance. Microsoft, Redmond. Https://technet.microsoft.com/en-us/library/jj203547.aspx. Luettu 14.1.2018.

Gaehtgens, Felix & Carpenter, Perry & Iverson, Brian & Kampman, Kevin 2017. Magic Quadrant for Identity Governance and Administration. Gartner, Stamford. Https://www.gartner.com/doc/reprints?id=1-3U2ZUET&ct=170222&st=sb. Luettu 14.1.2018.

Gibbs, Pervez 2015. SaaS vs. traditional software – What do you really need to know? Condeco, London. Http://blog.condecosoftware.com/saas-vs.-traditional-software-what-do-you-really-need-to-know. Luettu 8.9.2017.

Henkilötietolaki 22.4.1999/523.

Hintsanen, Kimmo 2014. Hallintatunnusten haasteet voi kohdata – katsaus ratkaisuun nimeltä Privileged Account Management | Nixu Oyj - Cybersecurity.

Https://www.nixu.com/fi/blogi/2014-12/hallintatunnusten-haasteet-voi-kohdata-katsauspam. Luettu 13.8.2017.

Hirsjärvi, Sirkka & Hurme, Helena 2008. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Gaudeamus Helsinki University Press, Helsinki.

Iverson, Brian 2015. Identity Governance and Administration: How We Got Here. Gartner, Stamford. Https://blogs.gartner.com/brian-iverson/2015/03/05/identity-governance-administration-got. Luettu 14.1.2018.

Jaakkola, Elina & Orava, Markus & Varjonen, Virpi 2009. Palvelujen tuotteistamisesta kilpailuetua. Opas yrityksille. 4. painos. Tekes, Helsinki.

Kamensky, Mika 2014. Strateginen johtaminen. Menestyksen timantti. 4., tarkistettu painos. Talentum, Helsinki.

Kananen, Jorma 2014. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylän ammattikorkeakoulu, Jyväskylä.

Kavanagh, Kelly M. & Bussa, Toby 2017. Magic Quadrant for Security Information and Event Management. Gartner, Stamford.

Kinnunen, Ritva 2004. Palvelujen suunnittelu. WSOY, Helsinki.

Kreizman, Gregg & Wynne, Neil 2016. Magic Quadrant for Identity and Access Management as a Service, Worldwide. Gartner, Stamford. Https://www.gartner.com/doc/reprints?id=1-38VVK6B&ct=160607&st=sb. Luettu 26.8.2017.

Kuhn, D. Richard & Coyne, Edward J. & Weil, Timothy R. 2010. Adding Attributes to Role-Based Access Control. IEEE Computer, vol. 43, no. 6 (June, 2010), 79-81. Http://csrc.nist.gov/groups/SNS/rbac/documents/kuhn-coyne-weil-10.pdf. Luettu 31.8.2017.

Kuntaliitto 2013a. Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri. Versio 1.0. Kuntaliitto, Helsinki.

Kuntaliitto 2013b. Kuntasektorin MDM-viitearkkitehtuuri. Versio 1.0. Kuntaliitto, Helsinki.

Laalo, Kari 2017. Luottamusverkko – Haka-käyttäjätunnistusjärjestelmä – Eduuni-wiki. Https://wiki.eduuni.fi/display/CSCHAKA/Luottamusverkko. Luettu 2.8.2017.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 7.8.2009/617.

Le Bras, Tom 2017. Do we have too many passwords? Https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought. Luettu 29.10.2017.

Lehtinen, Uolevi & Niinimäki, Satu 2005. Asiantuntijapalvelut. Tuotteistamisen ja markkinoinnin suunnittelu. WSOY, Helsinki.

Linden, Mikael 2011. Identiteetin- ja pääsynhallinta. Seminaariraportti. Seminaari, Tietojenkäsittelyn turvallisuus. Tampereen teknillinen yliopisto, Tampere.

Linden, Mikael 2015. Identiteetin- ja pääsynhallinta. Raportti 6. Tampereen teknillinen yliopisto, Tampere.

Lindqvist, Pekka 2018. Myyntijohtaja. Finceptum Oy, Espoo. Sähköposti 5.1.2018.

Lipsman, Effi 2017. Top 7 Reasons Why Your SIEM Project Is Failing. IntelliGO Networks Inc, Toronto. Http://www.intelligonetworks.com/blog/siem-7-reasons. Luettu 11.1.2018.

Matthing, Jonas & Sandén Bodil & Edvardsson, Bo 2004. New service development: learning from and with customers. International Journal of Service Industry Management. Vol. 15 Issue: 5, 479–498.

Mäntykangas, Ilpo 2017. Security Lead. Citrus Solutions Oy, Helsinki. Sähköposti 30.8.2017.

Mäntykangas, Ilpo 2018a. Security Lead. Citrus Solutions Oy, Helsinki. Sähköposti 11.1.2018.

Mäntykangas, Ilpo 2018b. Security Lead. Citrus Solutions Oy, Helsinki. Sähköposti 15.1.2018.

Mäntykangas, Ilpo 2018c. Security Lead. Citrus Solutions Oy, Helsinki. Sähköposti 6.2.2018.

Nikols, Nick 2017. CA Technologies. Five identity-centric cybersecurity shifts for 2017. Https://www.ca.com/en/blog-highlight/five-identity-centric-cybersecurity-shifts-2017.html. Luettu 29.10.2017.

Oikeusministeriö 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriö, Helsinki.

Ojansalo, Katri & Moilanen, Teemu & Ritalahti, Jarmo 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 3.–4. painos. Sanoma Pro Oy, Helsinki.

Parantainen, Jari 2007. Rakenna palvelusta tuote 10 päivässä. Tuotteistaminen. Talentum, Helsinki.

Pfleeger, Charles P. & Pfleeger, Shari Lawrence & Margulies, Jonathan 2015a. Security in Computing, Fifth Edition. ProQuest Safari Tech Books Online. Http://proquest-combo.safaribooksonline.com.ezproxy.metropolia.fi/book/networking/security/9780134085074/2dot-toolbox-authentication-access-control-and-cryptography/ch02lev1sec1_html. Luettu 5.12.2017.

Pfleeger, Charles P. & Pfleeger, Shari Lawrence & Margulies, Jonathan 2015b. Security in Computing, Fifth Edition. ProQuest Safari Tech Books Online. Http://proquest-combo.safaribooksonline.com.ezproxy.metropolia.fi/book/networking/security/9780134085074/2dot1-authentication/ch02lev2sec1_html. Luettu 5.12.2017.

Pfleeger, Charles P. & Pfleeger, Shari Lawrence & Margulies, Jonathan 2015c. Security in Computing, Fifth Edition. ProQuest Safari Tech Books Online. Http://proquest-combo.safaribooksonline.com.ezproxy.metropolia.fi/book/networking/security/9780134085074/2dot2-access-control/ch02lev2sec8_html. Luettu 5.12.2017.

Pfleeger, Charles P. & Pfleeger, Shari Lawrence & Margulies, Jonathan 2015d. Security in Computing, Fifth Edition. ProQuest Safari Tech Books Online. Http://proquest-combo.safaribooksonline.com.ezproxy.metropolia.fi/book/networking/security/9780134085074/2dot2-access-control/ch02lev2sec11_html. Luettu 5.12.2017.

Pfleeger, Charles P. & Pfleeger, Shari Lawrence & Margulies, Jonathan 2015e. Security in Computing, Fifth Edition. ProQuest Safari Tech Books Online. Http://proquest-combo.safaribooksonline.com.ezproxy.metropolia.fi/book/networking/security/9780134085074/8dot-cloud-computing/ch08lev1sec4_html. Luettu 5.12.2017.

Pfleeger, Charles P. & Pfleeger, Shari Lawrence & Margulies, Jonathan 2015f. Security in Computing, Fifth Edition. ProQuest Safari Tech Books Online. Http://proquest-combo.safaribooksonline.com.ezproxy.metropolia.fi/book/networking/security/9780134085074/8dot4-cloud-identity-management/ch08lev2sec10_html. Luettu 5.12.2017.

Pfleeger, Charles P. & Pfleeger, Shari Lawrence & Margulies, Jonathan 2015g. Security in Computing, Fifth Edition. ProQuest Safari Tech Books Online. Http://proquest-combo.safaribooksonline.com.ezproxy.metropolia.fi/book/networking/security/9780134085074/2dot2-access-control/ch02lev2sec9_html. Luettu 5.12.2017.

Ponemon Institute 2017. 2017 Cost of Data Breach Study. Global Overview. Ponemon Institute LLC, Michigan.

Ries, Eric 2011. The Lean Startup. Crown Business, New York.

Rissanen, Tapio 2006. Hyvän palvelun kehittäminen. Kustannusosakeyhtiö Pohjantähti PoleStar Ltd, Vaasa.

Rochford, Oliver & Kavanagh, Kelly M. & Bussa Toby 2016. Critical Capabilities for Security Information and Event Management. Gartner, Stamford. Https://www.gartner.com/doc/reprints?id=1-2Q17LAL&ct=151019&st=sb. Luettu 31.8.2017.

Savolainen, Jukka 2014. EU:n yleinen tietosuoja-asetus pakottaa julkisyhteisöt ja yritykset muuttamaan toimintamallejaan. Https://www-edilex-fi.ezproxy.metropolia.fi/uutiset/40278. Edilex. Luettu 7.12.2017.

Sipilä, Jorma 1996. Asiantuntijapalvelujen tuotteistaminen. WSOY, Porvoo.

Stackpole, Bill & Hanrion, Patrik 2007. Software Deployment, Updating, and Patching. CRC Press, Boca Raton.

Taiminen, Pasi 2018. Principal Consultant. Citrus Secure Identity Oy, Helsinki. Haastattelu 5.1.2018.

Tietoyhteiskuntakaari 7.11.2014/917.

Tuomi, Jouni & Sarajärvi, Anneli 2002. Laadullinen tutkimus ja sisällönanalyysi. Tammi, Helsinki.

Tuominen, Tiina & Järvi, Katriina & Lehtonen, Mikko H. & Valtanen, Jesse & Martinsuo, Miia 2015. Palvelujen tuotteistamisen käsikirja. Osallistavia menetelmiä palvelujen kehittämiseen. Aalto-yliopisto, Helsinki.

Valtakoski, Aku & Järvi, Katriina 2016. Productization of knowledge-intensive services: Enabling knowledge sharing and cross-unit collaboration. Journal of Service Management. Vol. 27 Issue: 3, 360–390.

Valtiovarainministeriö 2006. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. Valtionhallinnon tietoturvallisuuden johtoryhmä – VAHTI 9/2006. Valtiovarainministeriö, Helsinki.

Valtiovarainministeriö 2008. Valtionhallinnon tietoturvasanasto. Valtionhallinnon tietoturvallisuuden johtoryhmä – VAHTI 8/2008. Valtiovarainministeriö, Helsinki.

Valtiovarainministeriö 2009. Lokiohje. Valtionhallinnon tietoturvallisuuden johtoryhmä – VAHTI 8/2008. Valtiovarainministeriö, Helsinki.

Valtiovarainministeriö 2016a. EU-tietosuojan kokonaisuudistus. VAHTI-raportti – 1/2016. Valtiovarainministeriö, Helsinki.

Valtiovarainministeriö 2016b. Henkilöstön ja johdon tietoturvabarometri. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI 3/2016. Valtiovarainministeriö, Helsinki.

Valtori 2016. Kertakirjautumisratkaisu Virtu | Valtori. Http://www.valtori.fi/fi-Fi/Palvelut/Tietojarjestelmapalvelut/Identiteetin_ja_paasynhallinnan_palvelut/Kertakirjautumisratkaisu_Virtu. Päivitetty 30.12.2016. Luettu 6.2.2018.

Valtori 2017. Identiteetinhallintapalvelu Avain | Valtori. Http://www.valtori.fi/fi-FI/Palvelut/Tietojarjestelmapalvelut/Identiteetin_ja_paasynhallinnan_palvelut/Identiteetinhallintapalvelu_Avain/Identiteetinhallintapalvelu_Avain(3161). Päivitetty 7.4.2017. Luettu 8.12.2017.

Verizon 2017. 2017 Data Breach Investigations Report. 10th Edition.

Viestintävirasto 2016. Viestintäviraston teknisen ohjauksen katsaus 1/2016. Viestintävirasto, Helsinki.

Villanen, Jaana 2016. Tuotteista tähtituotteita. Kauppakamari, Helsinki.

Wagner, Ray & Allan, Ant & Gaehtgens, Felix & Kreizman, Gregg & Singh, Anmol & Perkins, Earl 2015. Predicts 2016: Identity and Access Management. Gartner, Stamford.

Haastattelun saate

Hei,

Opiskelen Metropolia Ammattikorkeakoulussa liiketaloutta monimuoto-opiskelijana. Olen aloittanut opinnäytetyön tekemisen, jonka teen toimeksiantajalle, Citrus Solutions Oy:lle. Opinnäytetyön aiheena on, osana toimeksiantajan identiteetin- ja pääsynhallinnan tuotteistamisprojektia, selvittää ja varmistaa asiakastarpeet sekä niiden perusteella arvioida alustavasti valittujen tuotteiden soveltuvuus asiakastarpeiden täyttämiseksi.

Ymmärtääkseni toimeksiantaja on ollut teihin yhteydessä koskien mahdollisia haastatteluita, joilla kyseiset asiakastarpeet on tarkoitus selvittää. Haastattelut tehdään joko henkilökohtaisesti kasvotusten tai etänä, käyttämällä esimerkiksi Skype for Business-sovellusta. Haastattelut tallennetaan digitaaliseen muotoon ja sen pohjalta tehdään yhteenveto. Yhteenveto toimitetaan haastattelun jälkeen haastateltavalle sähköpostitse. Haastattelut ovat luottamuksellisia ja niistä kertyvä aineisto on vain haastattelijan käytettävissä. Aineiston tuloksia käsitellään anonyymisti, joten yksittäisiä vastaajia ei voi tunnistaa aineistosta.

Haastattelussa käsiteltävät teemat ovat:

- Kertakirjautuminen (SSO), pilvipalvelut ja salasanat
- Tunnusten perustaminen ja poistaminen omiin sekä ulkopuolisiin palveluihin
- Identiteettien ja master datan hallinta
- Käyttäjien roolien ja käyttöoikeuksien myöntäminen automaattisesti
- EU:n tietosuoja-asetus (GDPR)
- Lokitietojen keskitetty kerääminen ja hallinta (SIEM)
- Ylläpitotunnusten hallintajärjestelmä (PAM)
- Luottamusverkostot (federaatiot)

Jotta voitte paremmin varautua haastatteluun, olen liittänyt mukaan liitteen, josta löydätte haastattelun aikana käsiteltäviä kysymyksiä eri teemoihin liittyen.
Jokainen haastattelu on opinnäytetyön onnistumisen kannalta erittäin tärkeä. Lisäksi se auttaa tuottamaan teille mahdollisimman hyvin teidän tarpeisiin vastaavaa palvelua. Toivottavasti löydämme yhteisen ajan haastattelun suorittamiseksi.

Ystävällisin terveisin,
Tommi Marjomaa

Haastattelun teemat ja käsiteltävät kysymykset

SSO, pilvipalvelut ja salasanat

* Onko teillä käytössänne useita eri pilvipalveluita?
* Mitä? / Voitteko kertoa miksi ette käytä pilvipalveluita?
* Käyttääkö henkilökunta pilvipalveluita myös omilla laitteillaan? Millä laitteilla?
* Millaisia haasteita henkilökunnalla on ollut pilvipalveluiden käytön kanssa?
* Millaisia tulevaisuuden näkymiä teillä on pilvipalveluiden käytön suhteen?
* Mitä/millaisia palveluita teillä on käytössänne, joiden kanssa tulisi käyttää vahvaa tunnistautumista?
* Voitteko kuvailla millainen olisi mahdollisimman toimiva SSO-palvelu pilvipalveluiden käytön helpottamiseksi?
* Onko teillä käytössä salasanojen resetoinnissa itsepalveluportaali?
* Millainen? / Oletteko ajatelleet hankkia sellaisen?
* Millaisia käyttökokemuksia teillä on sen suhteen?
* Millaisia kehitystarpeita teillä on sen suhteen?
* Voitteko kuvailla millainen olisi mahdollisimman toimiva itsepalveluportaali?
* Tuleeko teille jotain muuta mieleen aiheeseen liittyen minkä haluaisitte nostaa esille?

Tunnusten provisiointi ja deprovisiointi omiin ja ulkopuolisiin palveluihin

* Onko teillä käytössänne joku järjestelmä käyttäjätunnusten automaattiseen perustamiseen ja lopettamiseen?
* Millainen? / Oletteko suunnitelleet hankkia sellaisen?
* Millaisen järjestelmän hankkimista olette suunnitelleet?
* Tapahtuvatko muutokset reaaliajassa vai ajastettuina?
* Millaisia haasteita teillä on käyttäjätunnusten hallinnan kanssa?
* Mihin järjestelmiin ette saa perustettua tai lopetettua tunnuksia automaattisesti?
* Voitteko kuvailla minkälainen järjestelmä olisi mahdollisimman toimiva teidän tarpeisiinne?
* Millaisia käytäntöjä teillä on käyttäjätunnusten auditointien kanssa?
* Tuleeko teille jotain muuta mieleen aiheeseen liittyen minkä haluaisitte nostaa esille?

Identiteettien ja master datan hallinta

* Onko teillä käytössä master data-järjestelmää, jonka kautta käyttäjien valtuuksia ja attribuutteja voidaan hallinnoida?
* Millainen järjestelmä teillä on käytössä? / Oletteko suunnitelleet hankkia sellaisen?
* Millaisen järjestelmän hankkimista olette suunnitelleet?
* Millaisia haasteita teillä on master datan hallinnan kanssa?
* Ovatko kaikki järjestelmät liitetty master data-järjestelmään?
* Millaiset järjestelmät on liitetty master data-järjestelmään?
* Millaiset järjestelmät eivät ole liitetty master data-järjestelmään?
* Oletteko suunnitelleet kyseisten järjestelmien liittämistä master data-järjestelmään?
* Hallinnoidaanko näissä järjestelmissä samojen käyttäjien tietoja?
* Joudutaanko samoja tietoja päivittämään useissa eri järjestelmissä?
* Miten näistä haasteista voitaisiin päästä eroon?
* Voitteko kuvailla minkälainen järjestelmä olisi mahdollisimman toimiva teidän tarpeisiinne?
* Tuleeko teille jotain muuta mieleen aiheeseen liittyen minkä haluaisitte nostaa esille?

Roolien ja käyttöoikeuksien myöntäminen automaattisesti
* Onko teillä käytössä järjestelmä jonka kautta käyttäjien roolit ja käyttöoikeudet myönnetään automaattisesti eri järjestelmiin?
* Millainen järjestelmä teillä on käytössä? / Oletteko suunnitelleet hankkia sellaisen?
* Millaisia haasteita teillä on käyttäjäoikeuksien hallinnan kanssa?
* Millaisia käytäntöjä teillä on käyttäjäoikeuksien auditointien kanssa?
* Millaisia käytäntöjä teillä on käyttäjäoikeuksien myöntämisten ja muuttamisten jäljitettävyyden suhteen?
* Voitteko kuvailla minkälainen järjestelmä olisi mahdollisimman toimiva teidän tarpeisiinne?
* Tuleeko teille jotain muuta mieleen aiheeseen liittyen minkä haluaisitte nostaa esille?

GDPR
* Oletteko tietoinen EU:n uudesta tietosuoja-asetuksesta?
* Oletteko tietoinen sen asettamista vaatimuksista henkilötietojen käsittelyn osalta?
* Käsitelläänkö teillä henkilötiedoiksi luettavia tietoja?
* Miten teillä on varauduttu EU:n tietosuoja-asetuksen vaatimukseen rekisterinpitäjän osoitusvelvollisuudesta koskien asetuksen noudattamista henkilötietojen käsittelyssä?
* Miten teillä on varauduttu EU:n tietosuoja-asetuksen vaatimukseen rekisterinpitäjän velvollisuuteen ilmoittaa henkilötietojen tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle?
* Tuleeko teille jotain muuta mieleen aiheeseen liittyen minkä haluaisitte nostaa esille?

SIEM
* Onko SIEM-järjestelmä teille tuttu käsite?
SIEM-järjestelmän avulla eri palveluiden, järjestelmien ja laitteiden tuottamat lokitiedot keskitetään yhteen paikkaan. Se mahdollistaa tiedon keruun useista toisistaan suoraan riippumattomista järjestelmistä. Järjestelmän avulla luodaan mahdollisuus havaita useista pienistä palasista koostuvia suurempia tapahtumia. Lisäksi lokitietojen keskitetyllä keräämisellä voidaan varmistaa tapahtumien kiistämättömyys sekä mahdollistetaan väärinkäytösten havaitseminen ja selvittäminen.
* Onko teillä SIEM-järjestelmä käytössä?
* Millaisia käyttökokemuksia teillä on järjestelmästä? / Oletteko suunnitelleet hankkia sellaisen?
* Millaisia käytäntöjä teillä on lokien keräämisen suhteen?
* Monestako järjestelmästä kerätään lokitietoa?
* Seurataanko lokeja säännöllisesti?
* Kuinka lokeja hyödynnetään?
* Ketkä lokeja seuraavat?
* Onko lokitiedot varmennettu? Miten?
* Onko lokitiedot suojattu? Miten?
* Millaisia käytäntöjä teillä on lokien automaattisen käsittelyn suhteen?
* Millaisia haasteita teillä on ollut lokien käsittelyn suhteen?
* Miten valvotte käyttäjien ja ohjelmistojen poikkeavaa käyttäytymistä?
* Voitteko kuvailla minkälainen järjestelmä olisi mahdollisimman toimiva teidän tarpeisiinne?
* Tuleeko teille jotain muuta mieleen aiheeseen liittyen minkä haluaisitte nostaa esille?

PAM

* Onko ylläpitotunnusten hallintajärjestelmä teille tuttu?
* Onko teillä ylläpitotunnusten hallintajärjestelmä käytössä?
* Millainen järjestelmä teillä on käytössä? / Oletteko suunnitelleet hankkia sellaisen?
* Saadaanko järjestelmän avulla jäljitettyä ylläpitotunnusten käytön?
* Saadaanko istunnot tallennettua?
* Onko järjestelmä liitetty SIEM-järjestelmään?
* Millaisia haasteita teillä on ylläpitotunnusten käytön suhteen?
* Onko teillä käytössä jaettuja ylläpitotunnuksia, joita käyttää useampi henkilö?
* Miten teillä on järjestetty jaettujen ylläpitotunnusten käytön jäljitettävyys?
* Voitteko kuvailla minkälainen järjestelmä olisi mahdollisimman toimiva teidän tarpeisiinne?
* Tuleeko teille jotain muuta mieleen aiheeseen liittyen minkä haluaisitte nostaa esille?

Federaatiot

* Onko federaatio eli luottamusverkosto teille tuttu käsite?

Esimerkiksi HAKA on korkeakoulujen ja yliopistojen välinen luottamusverkosto, jossa osapuolet muodostavat monenkeskisen luottamusverkoston. Virtu on valtion virastojen luottamusverkosto. Niissä osapuolet luottavat toisiinsa ja toistensa käyttäjiin ja mahdollistavat luottamusverkostoon kuuluvien käyttäjien käyttää toistensa palveluita. Luottamus voi myös olla vain kahdenvälinen. Se voi myös olla keskitetty luottamusverkosto, jossa luottamus perustuu verkostoa operoivan keskusorganisaation ympärille. Federaatiossa kotiorganisaation tietohallinto vastaa itse käyttäjätiedoista ja pystyy siten hallinnoimaan ulkoisten palveluiden käyttöä omasta hakemistosta käsin.

* Onko teillä tarvetta järjestelmälle jonka kautta asiakkaat ja yhteistyökumppanit voivat tunnistautua luottamusverkoston avulla?
* Onko teillä tällaista järjestelmää käytössä?
* Oletteko suunnitelleet sellaisen hankkimista?
* Millaisissa tilanteissa teillä on tullut vastaan tarve asiakkaiden ja yhteistyökumppaneiden tunnistautumiselle?
* Onko teillä sellaisia palveluita, joita yhteistyökumppanit voisivat käyttää luottamusverkoston avulla? Mitä/Millaisia palveluita?
* Miten yhteistyökumppanit käyttävät kyseisiä palveluita tällä hetkellä?
* Onko teillä sellaisia palveluita, joita yhteistyökumppaneidenne asiakkaat tarvitsevat? Mitä/Millaisia palveluita?
* Miten niiden käyttö on tällä hetkellä järjestetty?
* Käytättekö te sellaisia yhteistyökumppaneiden palveluita, joita voisi käyttää luottamusverkoston avulla? Mitä/Millaisia palveluita?
* Miten te käytätte kyseisiä yhteistyökumppaneiden palveluita tällä hetkellä?
* Millaisia haasteita teillä on käyttää yhteistyökumppaneiden palveluita tällä hetkellä?
* Voitteko kuvailla minkälainen järjestelmä olisi mahdollisimman toimiva teidän tarpeisiinne?
* Mitkä asiakkaat, yhteistyökumppanit ja yhteistyökumppaneiden asiakkaat olisi teidän mielestä tärkeintä saada tunnistettua luottamusverkoston kautta?
* Tuleeko teille jotain muuta mieleen aiheeseen liittyen minkä haluaisitte nostaa esille?

Lopuksi

* Oletetaan, että olette hankkimassa identiteetin- ja pääsynhallintapalvelua (IAM) SaaS-palveluna. Millaisella hinnoittelumallilla haluaisitte palvelun hankkia? (per käyttäjä/kk, per tapahtuma, per järjestelmä, per palvelu jne.)
* Tuleeko teille jotain muuta mieleen minkä haluaisitte nostaa esille?

Selvitys asiakastarpeista ja tuotteiden soveltuvuuden varmistamisesta.